



# User Manual

## 4G LTE Router

DWR-921

---

# Preface

D-Link reserves the right to revise this publication and to make changes in the content hereof without obligation to notify any person or organization of such revisions or changes.

## Trademarks

D-Link and the D-Link logo are trademarks or registered trademarks of D-Link Corporation or its subsidiaries in the United States or other countries. All other company or product names mentioned herein are trademarks or registered trademarks of their respective companies.

Copyright © 2013 by D-Link Corporation, Inc.

All rights reserved. This publication may not be reproduced, in whole or in part, without prior expressed written permission from D-Link Corporation, Inc.

---

# FCC Regulations

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

This device has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

The antenna(s) used for this transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

This device complies with FCC radiation exposure limits set forth for an uncontrolled environment. In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antenna shall not be less than 20cm (8 inches) during normal operation.

# Table of Contents

<b>Preface.....</b>	<b>i</b>
Trademarks .....	i
FCC Regulations .....	ii
<b>Product Overview.....</b>	<b>1</b>
Package Contents.....	1
System Requirements .....	1
Introduction .....	2
Hardware Overview .....	3
Rear Panel.....	3
Front Panel .....	4
LEDs .....	5
<b>Installation .....</b>	<b>6</b>
Connect to Your Network .....	6
Wireless Installation Considerations.....	7
<b>Configuration.....</b>	<b>8</b>
Web-based Configuration Utility.....	8
Setup.....	9
Internet.....	9
Internet Connection Setup Wizard.....	9
Manual Internet Connection Setup .....	12
Internet Connection .....	12
Static IP .....	13
Dynamic IP (DHCP).....	14
PPPoE .....	15
PPTP .....	17
L2TP .....	19
3G/4G .....	20
Wireless Settings.....	22
Wireless Connection Setup Wizard.....	22
Manual Wireless Connection Setup .....	24
Wireless Settings .....	25
Wireless Security Mode .....	26
Wi-Fi Protected Setup (WPS) .....	29
Network Settings .....	32
Router Settings .....	32
DHCP Server Settings .....	33
Message Service.....	34
SMS Inbox .....	34
Create Message .....	35
Advanced .....	36
Virtual Server.....	36
Application Rules.....	38
QoS Engine.....	39
MAC Address Filter .....	40
URL Filter.....	41
Outbound Filter.....	42
Inbound Filter .....	43
SNMP .....	44
Routing .....	45
Advanced Wireless .....	46

---

Advanced Network .....	48	Troubleshooting .....	<b>77</b>
Network Scan .....	49	Tips.....	79
Tools .....	50	Networking Basics .....	<b>80</b>
Admin .....	50	Check your IP address.....	80
Time .....	51	Statically Assign an IP address .....	81
Syslog.....	52	Technical Specifications .....	<b>82</b>
Email Settings .....	53		
System .....	54		
Firmware .....	55		
Dynamic DNS .....	56		
System Check.....	57		
Schedules .....	58		
Status .....	59		
Device Info .....	59		
Log .....	60		
Statistics .....	61		
Wireless .....	62		
Support .....	63		
<b>Connecting to a Wireless Network .....</b>	<b>64</b>		
Using Windows 7 .....	64		
Configuring Wireless Security .....	66		
Using Windows Vista™ .....	69		
Configuring Wireless Security .....	70		
Using Windows® XP .....	72		
Configure WEP .....	73		
Configure WPA-PSK.....	75		

# Product Overview

## Package Contents

- D-Link DWR-921 4G LTE Router
- Power Adapter
- Manual and Warranty on CD
- 2 3G/4G Antennas

**Note:** Using a power supply with a different voltage rating than the one included with the DWR-921 will cause damage and void the warranty for this product.

## System Requirements

- A compatible (U)SIM card with service.\*
- Computer with Windows, Mac OS, or Linux-based operating system with an installed Ethernet adapter
- Java-enabled browser such as Internet Explorer 6, Safari 4.0, Chrome 20.0, or Firefox 7 or above (for configuration)

\*Subject to services and service terms available from your carrier.

# Introduction

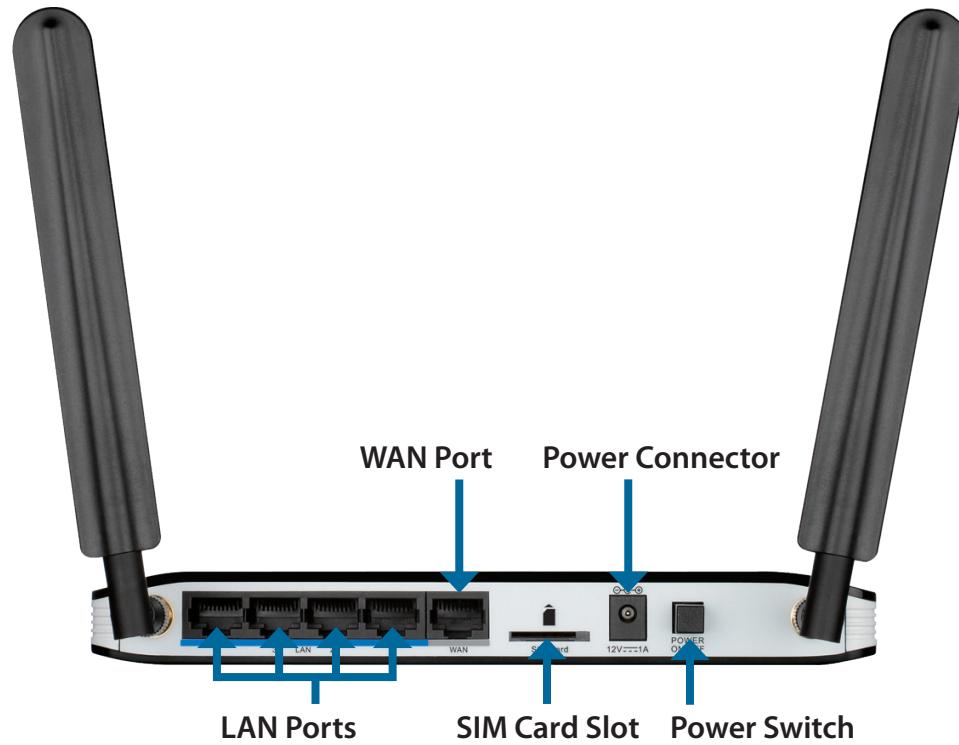
The D-Link 4G LTE Router allows users to access worldwide mobile broadband networks, and share them with a number of wired and wireless devices. Once connected, users can transfer data, stream media, and send SMS messages. Simply insert your UMTS/HSUPA SIM card, and share your 3G/4G Internet connection through a secure 802.11n wireless network or using any of the four 10/100 Ethernet ports.

The DWR-921 keeps your wireless network safe with WPA/WPA2 wireless encryption, preventing unauthorized users from accessing your network. The DWR-921 utilizes dual-active firewalls (SPI and NAT) to prevent potential attacks across the Internet, and includes MAC address filtering to control which clients can access your network, and what content they can access.

The DWR-921 4G LTE Router can be installed quickly and easily almost anywhere. This router is great for situations where an impromptu wireless network is required, or wherever conventional network access is unavailable. The DWR-921 can even be installed in buses, trains, or boats, allowing passengers to access the Internet while commuting.

# Hardware Overview

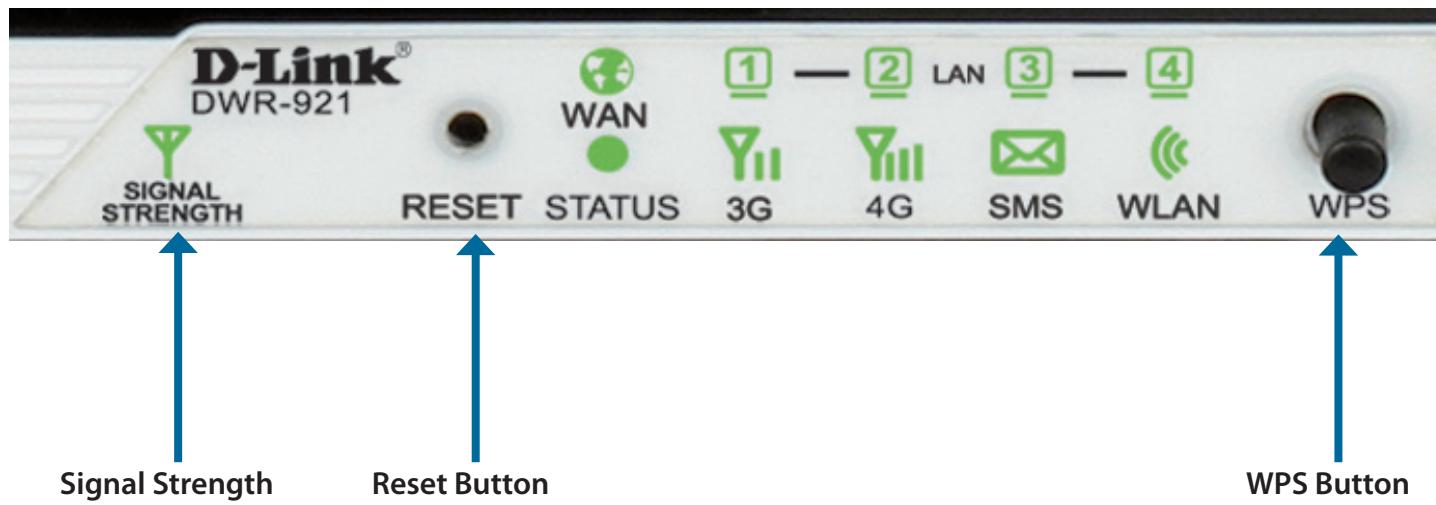
## Rear Panel



Port	Function
LAN Ethernet Ports	For connection to a network device such as a desktop or notebook computer.
WAN Ethernet Port	For connection to a DSL/Cable modem or router
SIM	Accepts a standard (U)SIM card for 3G/4G connectivity.
Power	Connects to the included power adapter.
Power Switch	Turns the device on or off.

# Hardware Overview

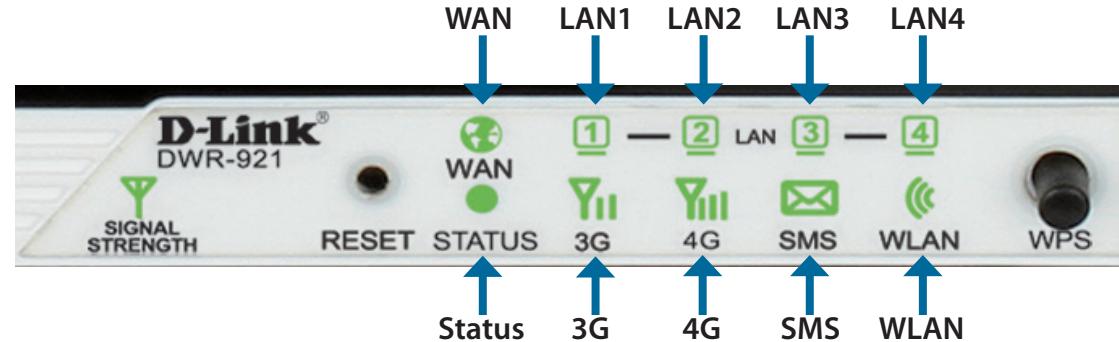
## Front Panel



Button Name	Function
Reset	Press this button with an unfolded paperclip to reset the device.
WPS	Press this button to initiate a new WPS connection. Refer to “Wi-Fi Protected Setup” on page 29 for more details.

# Hardware Overview

## LEDs



LED Name	Function
Signal Strength	Blinking Red: No SIM card/signal, or unverified PIN code Solid Red: Signal strength is at level one (weak) Solid Amber: Signal strength is at level two or three (medium) Solid Green: Signal strength is at level four or five (strong)
Status	Blinking Green: Device is powered on and working
WAN	Solid Green: Ethernet connection has been established Blinking Green: Data is being transferred
LAN 1-4	Solid Green: Ethernet connection has been established Blinking Green: Data is being transferred
3G	Solid Green: UMTS/HSDPA/HSUPA connection has been established Blinking Green: Data is being transferred via 3G
4G	Solid Green: LTE connection has been established Blinking Green: Data is being transferred via 4G
SMS	Solid Green: SMS storage is full Blinking Green: There is an unread SMS message
WLAN	Solid Green: WLAN is active and available Blinking Green: Data is being transferred over the WLAN

# Installation

This section will guide you through the installation process. Placement of the router is very important. Do not place the router in an enclosed area such as a closet, cabinet, or in an attic or garage.

## Connect to Your Network

1. Ensure that your DWR-921 4G LTE Router is disconnected and powered off.
2. Insert a standard (U)SIM card into the SIM card slot on the back of the router as indicated by the SIM card logo next to the slot. The gold contacts should face downwards.

**Caution:** Always unplug/power down the router before installing or removing the SIM card. Never insert or remove the SIM card while the router is in use.

3. Insert your Internet/WAN network cable into the WAN port on the back of the router.

**Note:** The 3G/4G connection can also be used as a backup WAN. Once a backup is configured, the router will automatically use 3G for the Internet connection if the Ethernet WAN is not available.

4. Insert the Ethernet cable into the LAN Port 1 on the back panel of the DWR-921 4G LTE Router and an available Ethernet port on the network adapter in the computer you will use to configure the router.

**Note:** The DWR-921 4G LTE Router LAN Ports are Auto-MDI/MDIX, so both patch and crossover Ethernet cables can be used.

5. Connect the power adapter to the power connector on the back panel of your DWR-921 4G LTE Router. Plug the other end of the power adapter into a wall outlet or power strip and turn the device on.
  - a. The Status LED will light up to indicate that power has been supplied to the router.
  - b. The LEDs on the front panel will flash on and off as the router performs initialization and Internet connection processes.
  - c. After a few moments, if a connection has been established, the following LEDs will turn solid green: Power, Status, WAN, WLAN, and any LAN Port LEDs that are connected to computers or other devices.

# Wireless Installation Considerations

The DWR-921 can be accessed using a wireless connection from anywhere within the operating range of your wireless network. Keep in mind that the quantity, thickness, and location of walls, ceilings, or other objects that the wireless signals must pass through may limit the range of the wireless signal. Ranges vary depending on the types of materials and background RF (radio frequency) noise in your home or office. The key to maximizing the wireless range is to follow these basic guidelines:

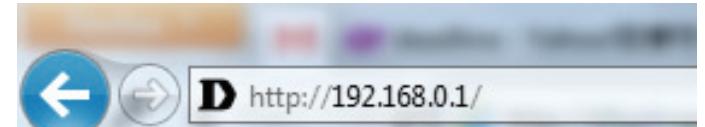
1. Minimize the number of walls and ceilings between the router and other network devices. Each wall or ceiling can reduce your adapter's range from 3 to 90 feet (1 to 30 meters).
2. Be aware of the direct line between network devices. A wall that is 1.5 feet thick (0.5 meters), at a 45-degree angle appears to be almost 3 feet (1 meter) thick. At a 2-degree angle it can appear over 42 feet (14 meters) thick. Position devices so that the signal will travel straight through a wall or ceiling (instead of at an angle) for better reception.
3. Try to position access points, wireless routers, and computers so that the signal passes through open doorways or drywall. Materials such as glass, metal, brick, insulation, concrete, and water can affect wireless performance. Large objects such as fish tanks, mirrors, filing cabinets, metal doors, and aluminum studs may also have a negative effect on range.
4. If you are using 2.4 GHz cordless phones, make sure that the phone base is as far away from your wireless device as possible. The base transmits a signal even if the phone is not in use. In some cases, cordless phones, X-10 wireless devices, and electronic equipment such as ceiling fans, fluorescent lights, and home security systems may dramatically degrade wireless connectivity.

# Configuration

This section will show you how to configure your new D-Link mobile router using the web-based configuration utility.

## Web-based Configuration Utility

To access the configuration utility, open a web browser such as Internet Explorer and enter the IP address of the router (192.168.0.1 by default).



To log in to the configuration utility, enter **admin** as the username, and then enter the password. By default, the password is blank.

If you get a **Page Cannot be Displayed** error, please refer to "Troubleshooting" on page 77 for assistance.

The configuration utility will open to the **STATUS > DEVICE INFO** page. You can view different configuration pages by clicking on the categories at the top of the screen (SETUP/ADVANCED/TOOLS/STATUS/SUPPORT), and then selecting a configuration page from the bar on the left side.

The following pages will describe each section in detail, starting with the **SETUP** pages.

A screenshot of the D-Link DWR-921 web-based configuration utility. The interface has a dark theme with orange highlights. At the top, there's a navigation bar with tabs for SETUP, ADVANCED, TOOLS, STATUS (which is selected), and SUPPORT. Below the navigation bar is a sidebar with links for DWR-921 //, DEVICE INFO, LOG, STATISTICS, WIRELESS, and LOGOUT. The main content area is divided into sections: DEVICE INFORMATION, GENERAL, and WAN. The DEVICE INFORMATION section displays connection details like Time (Sun Sep 16, 2012 22:06:03 -0800) and Firmware Version (V1.00, 2012/09/04). The GENERAL section shows a globe icon and a Reboot button. The WAN section shows Connection Type (DHCP Client) and Network Status (Established). On the right side, there's a sidebar with a 'Helpful hints...' section containing links for LAN/WAN and WIRELESS connection details, and a 'More...' link.

# Setup

The **SETUP** pages allow you to configure your Internet and wireless settings, as well as manage your SMS inbox. To view the Setup configuration pages, click on **SETUP** at the top of the screen.

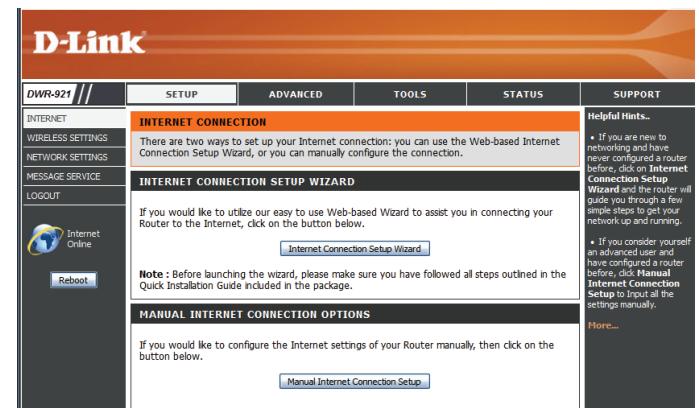


## Internet

The Internet page allows you to configure how your router connects to the Internet. There are two ways to set up your Internet connection.

You can click on the **Internet Connection Setup Wizard** button to start a wizard that will guide you through setting up your Internet settings.

If you want to manually configure your settings, click **Manual Internet Connection Setup** and skip to "Manual Internet Connection Setup" on page 12.

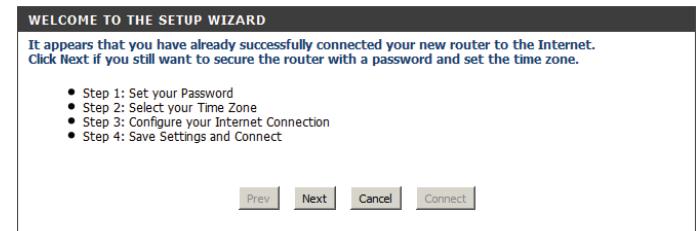


## Internet Connection Setup Wizard

This wizard will guide you through a step-by-step process to configure your router to connect to the Internet.

Click **Next** to continue.

**Note:** While using the wizard, you can click **Prev** to go back to the previous step, or you can click **Cancel** to close the wizard.



Create a new password and then click **Next** to continue.

**STEP 1: SET YOUR PASSWORD**

To secure your new networking device, please set and verify a password below:

Password :  Verify Password :

**Prev** **Next** **Cancel** **Connect**

Select your time zone from the drop-down box and then click **Next** to continue.

**STEP 2: SELECT YOUR TIME ZONE**

Select the appropriate time zone for your location. This information is required to configure the time-based options for the router.

(GMT-08:00) Pacific Time (US & Canada)

**Prev** **Next** **Cancel** **Connect**

Select the Internet connection type you use. The connection types are explained on the following page. If you are unsure which connection type you should use, contact your Internet Service Provider (ISP).

Click **Prev** to go back to the previous page or click **Cancel** to close the wizard.

**Note:** The DWR-921 has a WAN failover feature that allows the router to switch to a 3G/4G connection if the WAN connection is down or unavailable. To configure this feature, please refer to "Internet Connection" on page 12.

**STEP 3: CONFIGURE YOUR INTERNET CONNECTION**

Please select the Internet connection type below:

**DHCP Connection (Dynamic IP Address)**  
Choose this if your Internet connection automatically provides you with an IP Address. Most Cable Modems use this type of connection.

**Username / Password Connection (PPPoE)**  
Choose this option if your Internet connection requires a username and password to get online. Most DSL modems use this type of connection.

**Username / Password Connection (PPTP)**  
PPTP client.

**Username / Password Connection (L2TP)**  
L2TP client.

**3G/4G Connection**  
3G/4G.

**Static IP Address Connection**  
Choose this option if your Internet Setup Provider provided you with IP Address information that has to be manually configured.

**Prev** **Next** **Cancel** **Connect**

The subsequent configuration pages will differ depending on the selection you make on this page.

- DHCP Connection (Dynamic IP Address):** Choose this if your Internet connection automatically provides you with an IP address. Most cable modems use this type of connection. See "Dynamic IP (DHCP)" on page 14 for information about how to configure this type of connection.
- Username / Password Connection (PPPoE):** Choose this option if your Internet connection requires a username and password to connect. Most DSL modems use this style of connection. See "PPPoE" on page 15 for information about how to configure this type of connection.
- Username / Password Connection (PPTP):** Choose this option if your Internet connection requires Point-to-Point Tunneling Protocol (PPTP). See "PPTP" on page 17 for information about how to configure this type of connection.
- Username / Password Connection (L2TP):** Choose this option if your Internet connection requires Layer 2 Tunneling Protocol (L2TP). See "L2TP" on page 19 for information about how to configure this type of connection.
- 3G/4G Connection:** Choose this connection if you have installed a SIM card into the DWR-921. See "3G/4G" on page 20 for information about how to configure this type of connection.
- Static IP Address Connection:** Choose this option if your Internet Service Provider provided you with IP address information that has to be manually configured. See "Static IP" on page 13 for information about how to configure this type of connection.

After entering the requested information, click **Next** to continue.

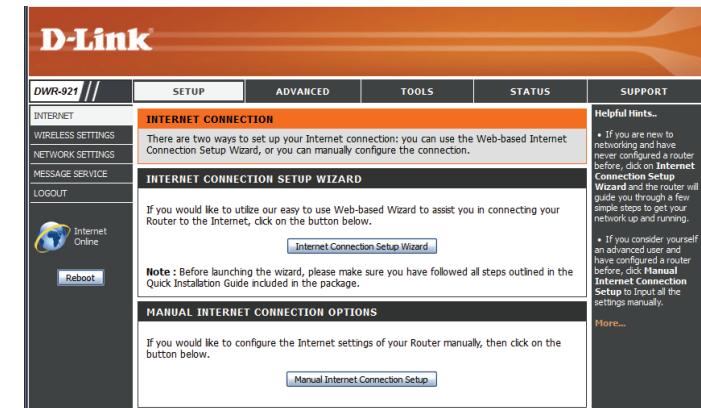
**Note:** If you are not sure what connection type to use or what settings to enter, check with your Internet Service Provider.

This completes the Internet Connection Setup Wizard. Click **Connect** to save your changes and reboot the router.



# Manual Internet Connection Setup

To set up your Internet connection manually, click **Manual Internet Connection Setup**.



## Internet Connection

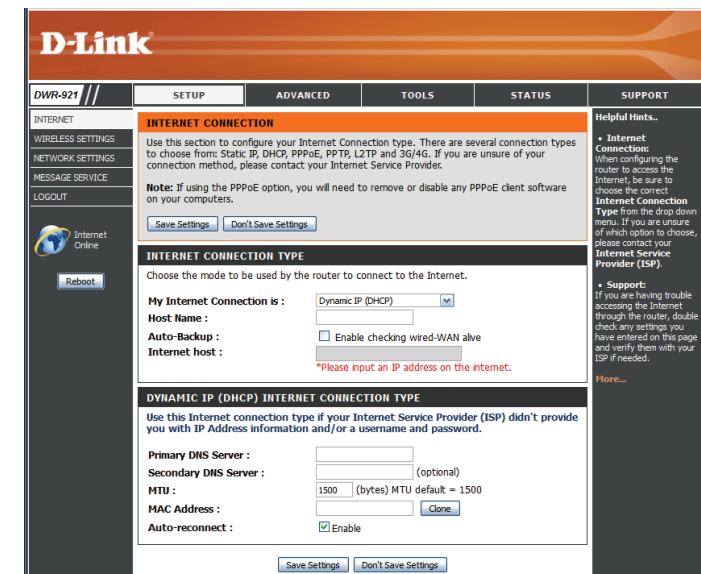
Several different Internet connection types can be selected depending upon the specifications of your Internet Service Provider (ISP). You can also set up the auto-backup feature, which allows you to use a 3G/4G connection for your Internet connection if your main connection fails.

**My Internet Connection is:** Select the Internet connection type specified by your ISP. The corresponding settings will be displayed below. Please see the following pages for details on how to configure these different connection types.

**Host Name:** If the Internet host you are using requires you to enter a host name, enter it here. In most cases, you may leave this blank.

**Auto-Backup:** If this feature is enabled, the router will switch over to a 3G/4G connection if the Internet host (specified below) is unreachable.

**Internet Host:** Enter an IP address for the router to use to check if it is connected to the Internet. If auto-backup is enabled and the IP address cannot be reached, the router will switch over to a 3G/4G connection.



## Static IP

Choose this Internet connection if your ISP assigns you a static IP address. After modifying any settings, click **Save Settings** to save your changes.

**IP Address:** Enter the IP address assigned to your network connection.

**Subnet Mask:** Enter the subnet mask.

**Default Gateway:** Enter the default gateway.

**Primary DNS Server:** Enter the primary DNS server.

**Secondary DNS Server:** Enter the secondary DNS server.

**MTU:** You may need to change the Maximum Transmission Unit (MTU) for optimal performance. The default value is 1500.

**MAC Address:** The default MAC address is set to the Internet port's physical interface MAC address on the broadband router. It is not recommended that you change the default MAC address unless required by your ISP. You can use the **Clone** button to replace the Internet port's MAC address with the MAC address of your Ethernet card.

STATIC IP ADDRESS INTERNET CONNECTION TYPE	
Enter the static address information provided by your Internet Service Provider (ISP).	
IP Address :	<input type="text"/>
Subnet Mask :	<input type="text"/>
Default Gateway :	<input type="text"/>
Primary DNS Server :	<input type="text"/>
Secondary DNS Server :	<input type="text"/>
MTU :	<input type="text"/> 1500 (bytes) MTU default = 1500
MAC Address :	<input type="text"/> <input type="button" value="Clone"/>

## Dynamic IP (DHCP)

This section will help you to obtain IP address information automatically from your ISP. Use this option if your ISP didn't provide you with IP address information and/or a username and password. After modifying any settings, click **Save Settings** to save your changes.

**Primary DNS Server:** (Optional) Fill in with IP address of primary DNS server.

**Secondary DNS Server:** (Optional) Fill in with IP address of secondary DNS server.

**MTU (Maximum Transmission Unit):** You may need to change the Maximum Transmission Unit (MTU) for optimal performance. The default value is 1500.

**MAC Address:** The default MAC Address is set to the Internet port's physical interface MAC address on the Broadband Router. It is not recommended that you change the default MAC address unless required by your ISP. You can use the **Clone** button to replace the Internet port's MAC address with the MAC address of your PC.

**Auto-reconnect:** This feature enables this product to renew the WAN IP address automatically when the lease time has expired.

The screenshot shows a configuration interface for 'DYNAMIC IP (DHCP) INTERNET CONNECTION TYPE'. It includes fields for 'Primary DNS Server' and 'Secondary DNS Server' (with a note '(optional)'), an 'MTU' field set to 1500 (bytes), a 'MAC Address' field with a 'Clone' button, and an 'Auto-reconnect' checkbox checked. At the bottom are 'Save Settings' and 'Don't Save Settings' buttons.

## PPPoE

Choose this Internet connection if your ISP provides you with a PPPoE account. After modifying any settings, click **Save Settings** to save your changes.

**Username:** The username/account name that your ISP provides to you for PPPoE dial-up.

**Password:** Password that your ISP provides to you for PPPoE dial-up.

**Verify Password:** Re-type your password in this field.

**Service Name:** Fill in if provided by your ISP. (Optional)

**IP Address:** Fill in if provided by your ISP. If not, keep the default value.

**Primary DNS Server:** Fill in if provided by your ISP. If not, keep the default value (optional).

**Secondary DNS Server:** Fill in if provided by your ISP. If not, keep the default value (optional).

**MAC Address:** MAC address of WAN interface. You can also copy MAC address of your PC to its WAN interface by clicking the **Clone** button.

**Maximum Idle Time:** The amount of time of inactivity before disconnecting an established PPPoE session. Set it to zero or enable auto-reconnect to disable this feature.

**PPPOE**  
Enter the information provided by your Internet Service Provider (ISP).

Username :	<input type="text"/>
Password :	<input type="password"/>
Verify Password :	<input type="password"/>
Service Name :	<input type="text"/> (optional)
IP Address :	<input type="text"/>
Primary DNS Server :	<input type="text"/> (optional)
Secondary DNS Server :	<input type="text"/> (optional)
MAC Address :	<input type="text"/>
Maximum Idle Time :	<input type="text"/> seconds
MTU :	<input type="text"/> 1492 (bytes) MTU default = 1492
Auto-reconnect :	<input type="checkbox"/> Enable

**Save Settings** **Don't Save Settings**

**Maximum Transmission Unit (MTU):** The default setting of PPPoE is 1492.

**Auto-reconnect:** The device will automatically reconnect to your PPPoE connection automatically.

**PPPOE**  
Enter the information provided by your Internet Service Provider (ISP).

Username :	<input type="text"/>
Password :	<input type="password"/>
Verify Password :	<input type="password"/>
Service Name :	<input type="text"/> (optional)
IP Address :	<input type="text"/>
Primary DNS Server :	<input type="text"/> (optional)
Secondary DNS Server :	<input type="text"/> (optional)
MAC Address :	<input type="text"/> <input type="button" value="Clone"/>
Maximum Idle Time :	<input type="text"/> seconds
MTU :	<input type="text"/> 1492 (bytes) MTU default = 1492
Auto-reconnect :	<input type="checkbox"/> Enable

## PPTP

Choose this Internet connection if your ISP provides you with a PPTP account. After modifying any settings, click **Save Settings** to save your changes.

**Address Mode:** Choose Static IP only if your ISP assigns you an IP address. Otherwise, please choose Dynamic IP.

**PPTP IP Address:** Enter the information provided by your ISP (Only applicable for Static IP PPTP).

**PPTP Subnet Mask:** Enter the information provided by your ISP (Only applicable for Static IP PPTP).

**PPTP Gateway IP Address:** Enter the information provided by your ISP (Only applicable for Static IP PPTP).

**PPTP Server IP Address:** IP address of PPTP server.

**Username:** User/account name that your ISP provides to you for PPTP dial-up.

**Password:** Password that your ISP provides to you for PPTP dial-up.

**Verify Password:** Re-enter your password for verification.

**Reconnect Mode:** Choose **Always-on** when you want to establish PPTP connection all the time. If you choose **Connect-on-demand**, the device will establish a PPTP connection when local users want to connect to the Internet, and disconnect if there is no traffic after the time period defined by the **Maximum Idle Time** setting.

The screenshot shows a configuration interface for PPTP. At the top, it says "Enter the information provided by your Internet Service Provider (ISP)". Below that, "Address Mode" is set to "Static IP". There are input fields for "PPTP IP Address", "PPTP Subnet Mask", "PPTP Gateway IP Address", and "PPTP Server IP Address". Below these are fields for "Username", "Password", and "Verify Password". Under "Reconnect Mode", "Always-on" is selected. The "Maximum Idle Time" is set to "300 seconds". At the bottom are "Save Settings" and "Don't Save Settings" buttons.

**Maximum Idle Time:** The time of no activity to disconnect your PPTP session. Set it to zero or choose **Always-on** to disable this feature.

**PPTP**  
Enter the information provided by your Internet Service Provider (ISP).

Address Mode :	<input type="radio"/> Dynamic IP <input checked="" type="radio"/> Static IP
PPTP IP Address :	<input type="text"/>
PPTP Subnet Mask :	<input type="text"/>
PPTP Gateway IP Address :	<input type="text"/>
PPTP Server IP Address :	<input type="text"/>
Username :	<input type="text"/>
Password :	<input type="text"/>
Verify Password :	<input type="text"/>
Reconnect Mode :	<input checked="" type="radio"/> Always-on <input type="radio"/> Connect-on-demand
Maximum Idle Time :	<input type="text" value="300"/> seconds

**Save Settings** **Don't Save Settings**

## L2TP

Choose this Internet connection if your ISP provides you with an L2TP account. After modifying any settings, click **Save Settings** to save your changes.

**Address Mode:** Choose **Static IP** only if your ISP assigns you an IP address. Otherwise, please choose **Dynamic IP**.

**L2TP IP Address:** Enter the information provided by your ISP  
(Only applicable for Static IP L2TP).

**L2TP Subnet Mask:** Enter the information provided by your ISP  
(Only applicable for Static IP L2TP).

**L2TP Gateway IP Address:** Enter the information provided by your ISP  
(Only applicable for Static IP L2TP).

**L2TP Server IP Address:** IP address of L2TP server.

**Username:** User/account name that your ISP provides to you for L2TP dial-up.

**Password:** Password that your ISP provides to you for L2TP dial-up.

**Verify Password:** Re-type your password in this field.

**Reconnect Mode:** Choose **Always-on** when you want to establish L2TP connection all the time. If you choose **Connect-on-demand** the device will establish L2TP connection when local users want to use Internet, and disconnect if no traffic after time period of Maximum Idle Time.

**Maximum Idle Time:** The time of no activity to disconnect your L2TP session. Set it to 0 or choose **Always-on** to disable this feature.

L2TP

Enter the information provided by your Internet Service Provider (ISP).

Address Mode :  Dynamic IP  Static IP

L2TP IP Address :

L2TP Subnet Mask :

L2TP Gateway IP Address :

L2TP Server IP Address :

Username :

Password :

Verify Password :

Reconnect Mode :  Always-on  Connect-on-demand

Maximum Idle Time : 300 seconds

Save Settings    Don't Save Settings

## 3G/4G

Choose this Internet connection if you already use a SIM card for 3G/4G Internet service from your mobile Internet service provider. The fields here may not be necessary for your connection. The information on this page should only be used if required by your service provider. After modifying any settings, click **Save Settings** to save your changes.

**Prefer Service Type:** Choose whether the DWR-921 should only use 4G networks, 3G networks, or use **Auto Mode** to automatically select a network.

**Dial Up Profile:** Select **Auto-Detection** to have the router automatically detect the settings for your connection. Select **Manual** to enter the details of your connection manually.

**Account/Profile Name:** Fill in a name to identify the following 3G/4G configuration.

**Country/Telecom:** Select your country and service provider to automatically fill in some of the required settings.

**Username:** Fill in only if requested by ISP (optional).

**Password:** Fill in only if requested by ISP (optional).

**Dialed Number:** Enter the number to be dialed.

**Authentication:** Select **PAP**, **CHAP**, or **Auto** detection. The default authentication method is **Auto**.

**APN:** Enter the APN information (optional).

**Pin Code:** Enter the PIN associated with your SIM card.

**Reconnect Mode:** Select **Auto** or **Manual** to determine whether the router should reconnect to your 3G/4G network automatically or manually.

The screenshot shows a configuration interface for a 3G/4G internet connection. The top bar has the title "3G/4G INTERNET CONNECTION TYPE" and a subtitle "Enter the information provided by your Internet Service Provider (ISP)". Below this, there are several groups of configuration options:

- Prefer Service Type:** A dropdown menu showing "Auto Mode" selected.
- Dial-Up Profile:** Radio buttons for "Auto-Detection" (selected) and "Manual".
- Country:** A dropdown menu showing "Angola" selected.
- Telecom:** A dropdown menu showing "Unitel" selected.
- Account/Profile Name:** An empty text input field.
- Username:** An empty text input field with "(optional)" note.
- Password:** An empty text input field with "(optional)" note.
- Verify Password:** An empty text input field with "(optional)" note.
- Dialed Number:** An empty text input field.
- Authentication:** A dropdown menu showing "Auto" selected.
- APN:** An empty text input field.
- Pin Code:** An empty text input field.
- Reconnect Mode:** Radio buttons for "Auto" (selected) and "Manual".
- Maximum Idle Time:** A text input field containing "300" followed by "seconds".
- Primary DNS Server:** An empty text input field.
- Secondary DNS Server:** An empty text input field.
- Keep Alive:** Radio buttons for "Disable" (selected) and "Use Ping".
- Bridge ethernet ports:** A checkbox that is unchecked.
- Roaming:** A checkbox that is unchecked.
- DNS check:** A checkbox that is unchecked.
- NAT disable:** A checkbox that is unchecked.

At the bottom right are two buttons: "Save Settings" and "Don't Save Settings".

**Maximum Idle Time:** Set the maximum time your connection can be idle before disconnecting. Set it to 0 or choose Auto in Reconnect Mode to disable this feature.

**Primary DNS Server:** Fill in if provided by your ISP. If not, keep the default value (optional).

**Secondary DNS Server:** Fill in if provided by your ISP. If not, keep the default value (optional).

**Keep Alive:** Select **Disable** or **Use Ping** depending on the settings required by your ISP. If you select Use Ping, set the ping interval and the IP address to ping.

**Bridge Ethernet Ports:** Activate this feature to use the Ethernet WAN port as an additional LAN port.

**Roaming:** Enabling this option will allow you to connect when roaming.

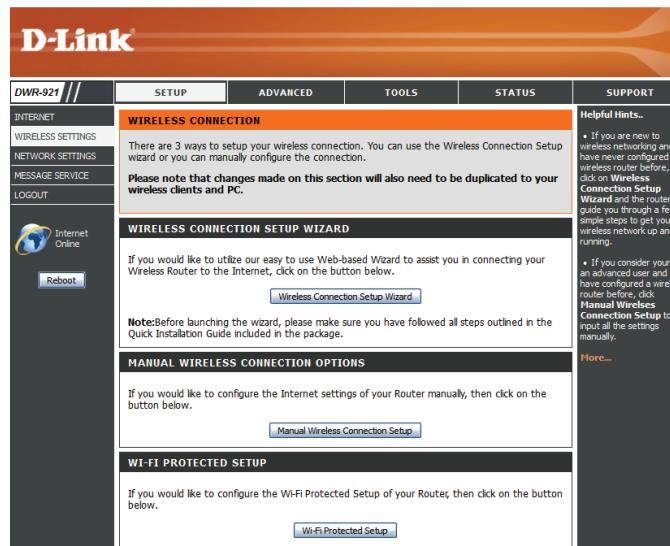
**Note:** Roaming connections may incur additional fees from your service provider.

**DNS Check:** Enabling this will send periodic DNS checks to make sure your connection is alive, and if the check fails, it will restart your 3G connection to resume connectivity.

**NAT Disable:** Enabling this option will disable the NAT function of the DWR-921, allowing it to act as a link for your devices to your Internet connection, but without routing functions.

# Wireless Settings

This section will help you to manually configure the wireless settings of your router. Please note that changes made in this section may also need to be duplicated on your wireless devices and clients. The Wireless Settings page allows you to configure how your router connects to the Internet. There are several ways to set up your wireless connection. You can click on the **Wireless Connection Setup Wizard** button to start a wizard that will guide you through setting up your wireless settings. If you want to manually configure your settings, click the **Manual Wireless Connection Setup** button and skip to “Manual Wireless Connection Setup” on page 24. You can also set up a wireless connection to a device automatically, or configure your router automatically through Windows by clicking the **Wi-Fi Protected Setup** button. This is described in “Wi-Fi Protected Setup (WPS)” on page 29.



## Wireless Connection Setup Wizard

This wizard will guide you through a step-by-step process to configure your router’s wireless .

Click **Next** to continue.

**Note:** While using the wizard, you can click **Prev** to go back to the previous page or you can click **Cancel** to close the wizard.



## Section 3 - Configuration

Enter a name (SSID) for your wireless network, then click **Next** to continue.

**STEP 1: NAME YOUR WIRELESS NETWORK**

Your wireless network needs a name so it can be easily recognized by wireless clients. For security purposes, it is highly recommended to change the pre-configured network name of [default].

Wireless Network Name (SSID) : myNetwork

Prev Next Cancel Save

Select a level of wireless security to use, then click **Next** to continue.

**STEP 2: SECURE YOUR WIRELESS NETWORK**

In order to protect your network from hackers and unauthorized users, it is highly recommended you choose one of the following wireless network security settings.

There are three levels of wireless security -Good Security, Better Security, or Best Security. The level you choose depends on the security features your wireless adapters support.

BEST :  Select this option if your wireless adapters SUPPORT WPA2  
BETTER :  Select this option if your wireless adapters SUPPORT WPA  
GOOD :  Select this option if your wireless adapters DO NOT SUPPORT WPA  
NONE :  Select this option if you do not want to activate any security features

For information on which security features your wireless adapters support, please refer to the adapters' documentation.

Note: All wireless adapters currently support WPA.

Prev Next Cancel Save

If you chose **BEST** or **BETTER**, select whether to use TKIP or AES encryption, then enter a password to use for your wireless network. It is recommended that you use AES if your wireless computers and devices support it, as it is more secure. Click **Next** to continue.

**STEP 3: SET YOUR WIRELESS SECURITY PASSWORD**

Once you have selected your security level - you will need to set a wireless security password. With this password, a unique security key will be generated.

Wireless Security Password :  AES  TKIP  myPassword

Note: You will need to enter the unique security  AES  TKIP generated into your wireless clients enable proper wireless communication - not the password you provided to create the security key.

Prev Next Cancel Save

If you chose **GOOD**, select whether to use a HEX or ASCII password, then enter a password to use for your wireless network. If you choose HEX, you will need to enter a 10 or 26 digit password using only hex characters (0-9, A-F). If you choose ASCII, the password must be 5 or 13 alphanumeric characters. Click **Next** to continue.

**STEP 3: SET YOUR WIRELESS SECURITY PASSWORD**

Once you have selected your security level - you will need to set a wireless security password. With this password, a unique security key will be generated.

Wireless Security Password :  HEX  ASCII  1234567890

Note: You will need to enter the unique security  HEX  ASCII generated into your wireless clients enable proper wireless communication - not the password you provided to create the security key.

Prev Next Cancel Save

This completes the Wireless Connection Setup Wizard. Click **Save** to save your changes and reboot the router.

**SETUP COMPLETE!**

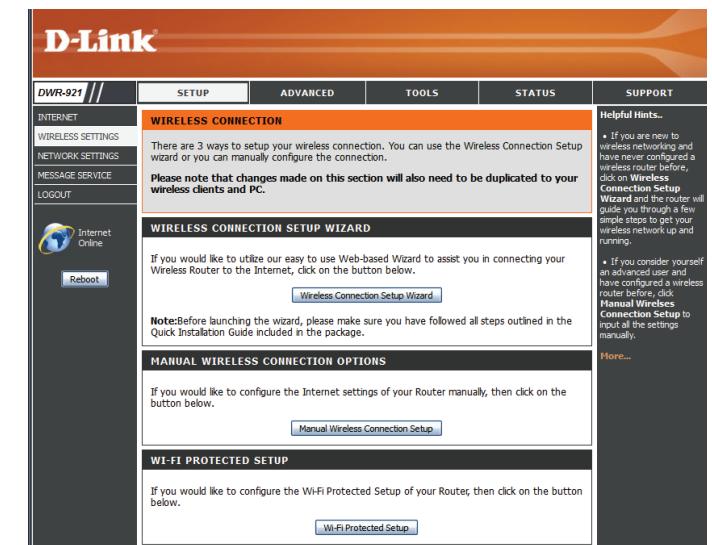
Below is a detailed summary of your wireless security settings. Please print this page out, or write the information on a piece of paper, so you can configure the correct settings on your wireless client adapters.

Wireless Network Name (SSID) : myNetwork

Prev Next Cancel Save

# Manual Wireless Connection Setup

To set up your wireless connection manually, click **Manual Wireless Connection Setup**.



# Wireless Settings

This page lets you set up your wireless network and choose a wireless security mode. After modifying any settings, click **Save Settings** to save your changes.

**Enable Wireless:** Check this box to enable wireless access. When you enable this option, the following parameters take effect.

**Wireless Network Name:** Also known as the SSID (Service Set Identifier), this is the name of your Wireless Local Area Network (WLAN). Enter a name using up to 32 alphanumeric characters. The SSID is case-sensitive.

**802.11 Mode:** **B/G mixed:** Enable this mode if your network contains a mix of 802.11b and 802.11g devices.

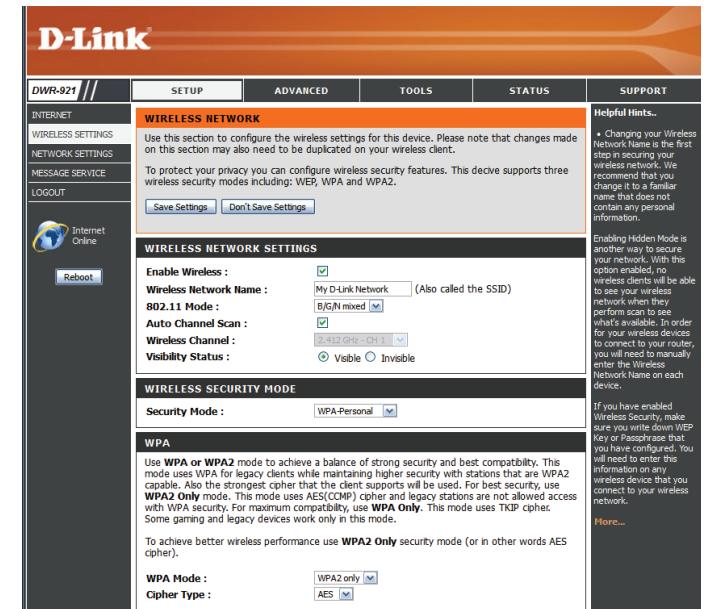
**N only:** Enable this mode if your network only has 802.11n devices.

**B/G/N mixed:** Enable this mode if you have a mix of 802.11n, 802.11g, and 802.11b clients.

**Auto Channel Scan:** Enabling this feature will allow the router to automatically scan for the best wireless channel to use.

**Wireless Channel:** A wireless network uses specific channels in the wireless spectrum to handle communication between clients. Some channels in your area may experience interference from other electronic devices. Choose the clearest channel to help optimize the performance and coverage of your wireless network, or enable Auto Channel Scan for the router to automatically select the best channel.

**Visibility Status:** This setting determines whether the SSID will be **Visible** or **Invisible** to wireless clients looking for wireless networks. Setting this to **Invisible** can increase the security of your network by making it undetectable, but clients will need to manually enter the SSID of your network to connect.

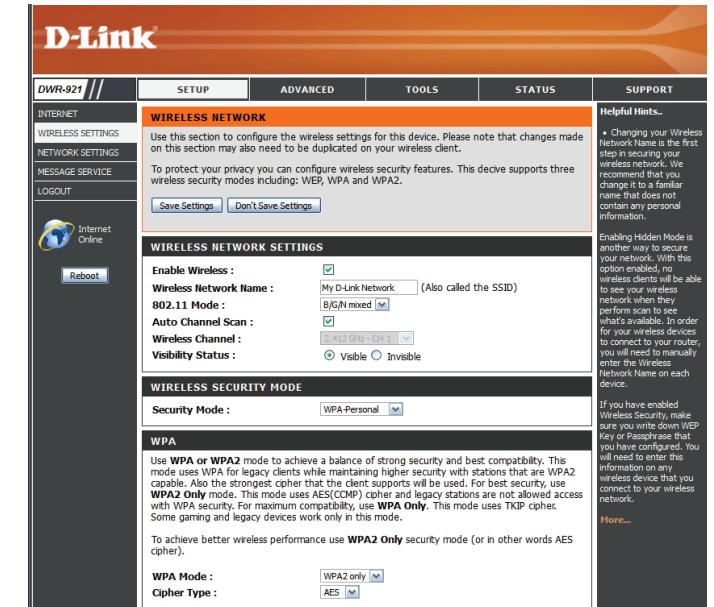


## Wireless Security Mode

You can choose from several different wireless security modes. After selecting a mode, the settings for that mode will appear. After modifying any settings, click **Save Settings** to save your changes.

**Security Mode:** You can choose from 4 different security modes.

- **None:** No security will be used. This setting is not recommended.
- **WEP:** WEP encryption will be used. This setting is only recommended if your wireless devices do not support WPA or WPA2.
- **WPA-Personal:** WPA-PSK encryption will be used. This setting is recommended for most users.
- **WPA-Enterprise:** WPA-EAP encryption will be used. This setting is only recommended if you have a RADIUS authentication server. Otherwise, **WPA-Personal** should be used.



If you choose **WEP**, the following options will appear:

**Authentication:** Select whether to use **Open** or **Shared** authentication.

**WEP Encryption:** Select whether to use **64-bit** or **128-bit** encryption.

**Default WEP Key:** Select which WEP key (1-4) to use as the default key. This will also change the WEP Key text box to that WEP key for your to configure(1-4).

**WEP Key:** Set the WEP key/password for your wireless network. Based on whether you are using 64 or 128-bit encryption, and whether you are using a HEX or ASCII key, you will need to enter different numbers of characters for your key, as indicated below the WEP Key text box. ASCII keys may use letters and numbers only, and HEX keys may use numbers 0-9 and letters A-F only.

WIRELESS SECURITY MODE	
Security Mode :	WEP
<b>WEP</b>	
WEP is the wireless encryption standard. To use it you must enter the same key(s) into the router and the wireless stations. For 64 bit keys you must enter 10 hex digits into each key box. For 128 bit keys you must enter 26 hex digits into each key box. A hex digit is either a number from 0 to 9 or a letter from A to F. For the most secure use of WEP set the authentication type to "Shared Key" when WEP is enabled.	
You may also enter any text string into a WEP key box, in which case it will be converted into a hexadecimal key using the ASCII values of the characters. A maximum of 5 text characters can be entered for 64 bit keys, and a maximum of 13 characters for 128 bit keys.	
Authentication :	Open
WEP Encryption :	64Bit
Default WEP Key :	WEP Key 1
WEP Key :	HEX <input checked="" type="checkbox"/> 1234567890 (5 ASCII or 10 HEX)

If you choose **WPA-Personal**, the following options will appear:

**WPA Mode:** Select whether to use **WPA2 only** or **WPA only**. **WPA2 only** is the most secure, provided that all of your clients can support it.

**Cipher Type:** Select whether to use the **TKIP** or **AES** cipher. The **AES** cipher is the most secure, provided that all of your clients can support it.

**Network Key:** Enter the key/password you want to use for your wireless network. The key must be between 8 and 63 characters long, and may only contain letters and numbers.

WIRELESS SECURITY MODE	
Security Mode :	WPA-Personal
<b>WPA</b>	
Use <b>WPA</b> or <b>WPA2</b> mode to achieve a balance of strong security and best compatibility. This mode uses WPA for legacy clients while maintaining higher security with stations that are WPA2 capable. Also the strongest cipher that the client supports will be used. For best security, use <b>WPA2 Only</b> mode. This mode uses AES(CMP) cipher and legacy stations are not allowed access with WPA security. For maximum compatibility, use <b>WPA Only</b> . This mode uses TKIP cipher. Some gaming and legacy devices work only in this mode.	
To achieve better wireless performance use <b>WPA2 Only</b> security mode (or in other words AES cipher).	
WPA Mode :	WPA only
Cipher Type :	AES
<b>PRE-SHARED KEY</b>	
Enter an 8- to 63-character alphanumeric pass-phrase. For good security it should be of ample length and should not be a commonly known phrase.	
Network Key :	7c9aeccad9c6b0c05343ed88747544b747ffd2 (8~63 ASCII or 64 HEX)

If you choose **WPA-Enterprise**, the following options will appear:

**WPA Mode:** Select whether to use **WPA2 only** or **WPA only**. **WPA2 only** is the most secure, provided that all of your clients can support this security method.

**Cipher Type:** Select whether to use the **TKIP** or **AES** cipher. The **AES** cipher is the most secure, provided that all of your clients can support it.

**RADIUS Server IP Address:** Enter the IP address of your RADIUS server.

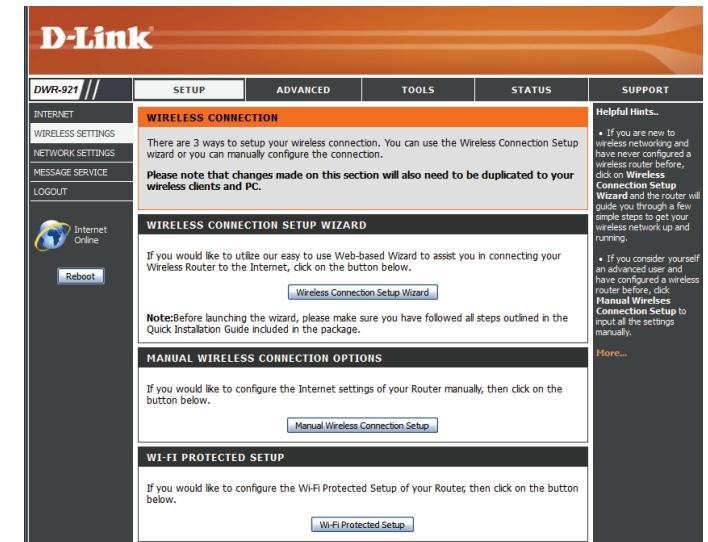
**RADIUS Server Port:** Enter the port used for your RADIUS server.

**RADIUS Server Shared Secret:** Enter the shared secret/password for your RADIUS server.

<b>WIRELESS SECURITY MODE</b>	
Security Mode : <input type="button" value="WPA-Enterprise"/>	
<b>WPA</b>	
Use <b>WPA</b> or <b>WPA2</b> mode to achieve a balance of strong security and best compatibility. This mode uses WPA for legacy clients while maintaining higher security with stations that are WPA2 capable. Also the strongest cipher that the client supports will be used. For best security, use <b>WPA2 Only</b> mode. This mode uses AES(CCMP) cipher and legacy stations are not allowed access with WPA security. For maximum compatibility, use <b>WPA Only</b> . This mode uses TKIP cipher. Some gaming and legacy devices work only in this mode.	
To achieve better wireless performance use <b>WPA2 Only</b> security mode (or in other words AES cipher).	
WPA Mode : <input type="button" value="WPA only"/>	
Cipher Type : <input type="button" value="AES"/>	
<b>EAP (802.1X)</b>	
When WPA enterprise is enabled, the router uses EAP (802.1x) to authenticate clients via a remote RADIUS server.	
RADIUS Server IP Address :	<input type="text" value="0.0.0.0"/>
RADIUS server Port :	<input type="text" value="1812"/>
RADIUS server Shared Secret :	<input type="text"/>

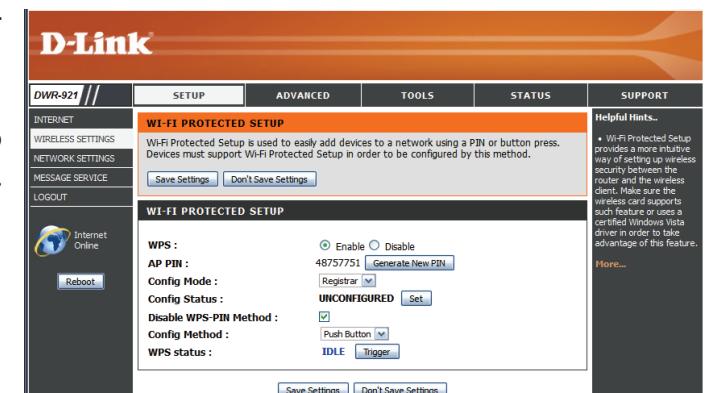
# Wi-Fi Protected Setup (WPS)

To open the Wi-Fi Protected Setup page, click **Wi-Fi Protected Setup**.

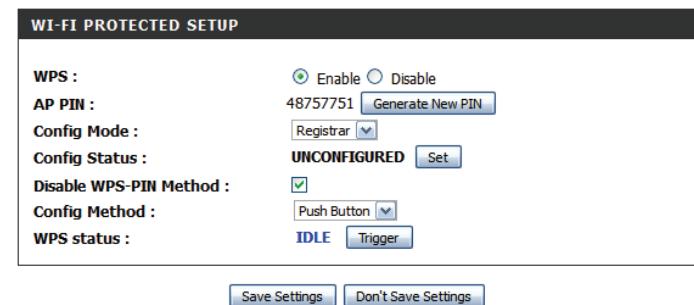


The Wi-Fi Protected Setup page allows you to create a wireless connection between your router and a device automatically by simply pushing a button or entering a PIN code.

You can also use Windows 7 to do initial configuration of your router by using the **Connect to a network** wizard in Windows, and entering the WPS PIN/AP PIN of the router when prompted. After modifying any settings, click **Save Settings** to save your changes.



- WPS:** Select whether you would like to **Enable** or **Disable** WPS features.
- AP PIN (also known as WPS PIN):** If you use Windows 7's **Connect to a network** wizard to do initial configuration of the router, you will need to enter the WPS PIN/AP PIN into the wizard when prompted. The factory default WPS PIN/AP PIN is printed on a label located on the bottom of the router. You can click the **Generate New PIN** button to change it to a randomly generated PIN.
- Config Mode:** Select whether the WPS config mode should be set to **Registrar** or **Enrollee**. In most cases, this should be set to **Registrar** so that you can use WPS to connect new wireless clients.
- Config Status:** If this is set to **CONFIGURED**, the router will be marked as "already configured" to computers that try to use WPS configuration, such as Windows 7's **Connect to a network** wizard. You can click the **Release** button to change the status to **UNCONFIGURED** to allow for WPS configuration of the router.
- If this is set to **UNCONFIGURED**, you can click the **Set** button to change the status to **CONFIGURED** to block WPS configuration of the router.
- Disable WPS Pin Method:** Enable this option to prevent clients from connecting to the router using the PIN method. If this option is enabled, clients must use the push-button method to connect.
- Config Method:** This lets you choose whether to use the **Push Button** connection method (PBC) or **PIN** method to connect to a wireless client when the **Trigger** button is clicked. If you choose the **PIN** method, you will need to enter an 8-digit PIN number that the wireless client needs to use to connect to your router.



**WPS Status:** This will show the current WPS connection process status. Click the **Trigger** button to initiate a WPS connection.

The screenshot shows a configuration interface for 'WI-FI PROTECTED SETUP'. It includes the following fields and options:

- WPS :** Radio buttons for 'Enable' (selected) and 'Disable'.
- AP PIN :** Text input field showing '48757751' with a 'Generate New PIN' button.
- Config Mode :** A dropdown menu currently set to 'Registrar'.
- Config Status :** Text field showing 'UNCONFIGURED' with a 'Set' button.
- Disable WPS-PIN Method :** A checked checkbox.
- Config Method :** A dropdown menu currently set to 'Push Button'.
- WPS status :** Text field showing 'IDLE' with a 'Trigger' button.

At the bottom are two buttons: 'Save Settings' and 'Don't Save Settings'.

# Network Settings

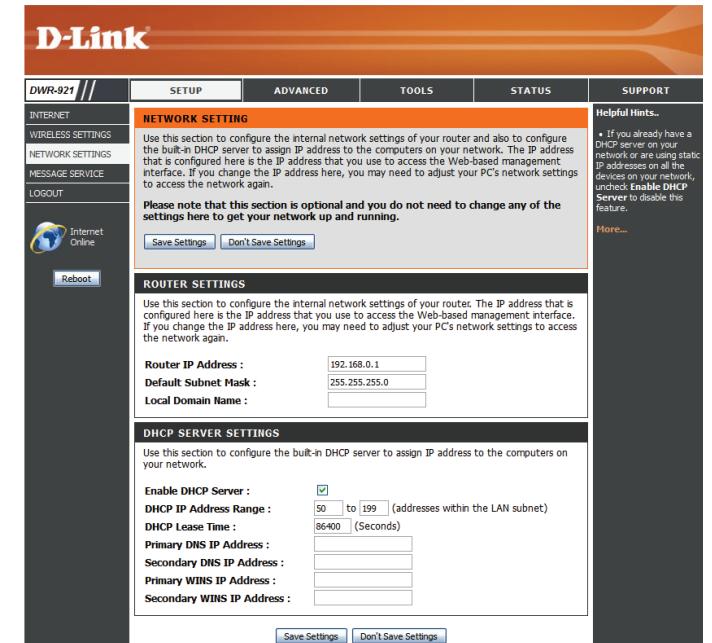
This section will help you to change the internal network settings of your router and to configure the DHCP Server settings. After modifying any settings, click **Save Settings** to save your changes.

## Router Settings

**Router IP Address:** Enter the IP address you want to use for the router. The default IP address is **192.168.0.1**. If you change the IP address, you will need to enter the new IP address in your browser to get into the configuration utility.

**Default Subnet Mask:** Enter the **Subnet Mask** of the router. The default subnet mask is **255.255.255.0**.

**Local Domain Name:** Enter the local domain name for your network.



## DHCP Server Settings

The DWR-921 has a built-in DHCP (Dynamic Host Control Protocol) server. The DHCP server assigns IP addresses to devices on the network that request them. By default, the DHCP Server is enabled on the device. The DHCP address pool contains a range of IP addresses, which are automatically assigned to the clients on the network. After modifying any settings, click **Save Settings** to save your changes.

**Enable DHCP Server:** Select this box to enable the DHCP server on your router.

**DHCP IP Address Range:** Enter the range of IPs for the DHCP server to use to assign IP addresses to devices on your network. These values will represent the last octet of the IP addresses in the pool.

**DHCP Lease Time:** Enter the lease time for IP address assignments.

**Primary DNS IP Address:** Enter the primary DNS IP address that will be assigned to DHCP clients.

**Secondary DNS IP Address:** Enter the secondary DNS IP address that will be assigned to DHCP clients.

**Primary WINS IP Address:** Enter the primary WINS IP address that will be assigned to DHCP clients.

**Secondary WINS IP Address:** Enter the secondary WINS IP address that will be assigned to DHCP clients.

**DHCP SERVER SETTINGS**

Use this section to configure the built-in DHCP server to assign IP address to the computers on your network.

Enable DHCP Server :

DHCP IP Address Range :  50 to  199 (addresses within the LAN subnet)

DHCP Lease Time :  86400 (Seconds)

Primary DNS IP Address :

Secondary DNS IP Address :

Primary WINS IP Address :

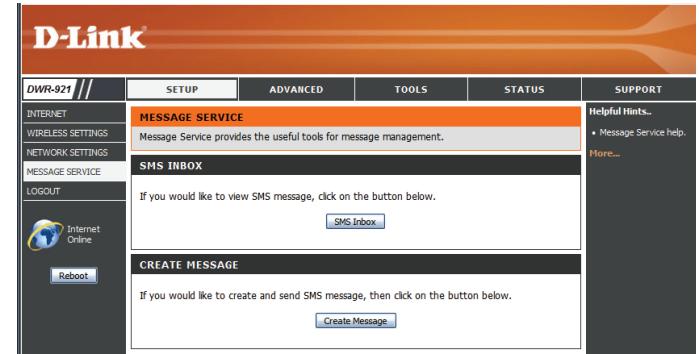
Secondary WINS IP Address :

Save Settings  Don't Save Settings

# Message Service

If your ISP provides **SMS** service, you can check and send messages from this page.

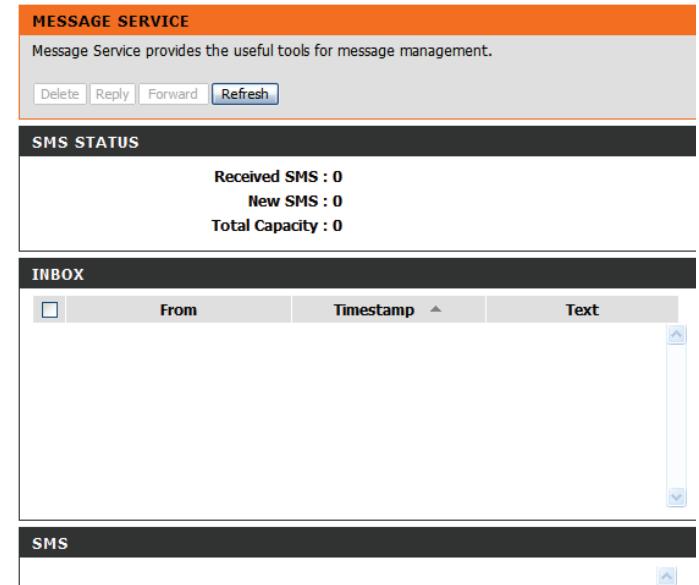
- SMS Inbox:** Click this button to view SMS messages that you have received.
- Create Message:** Click this button to create a new message to send.



## SMS Inbox

This page shows all messages that are stored on the SIM card. Select a message to display its contents in the SMS window. After you have read a message, you can delete it, or reply to the sender. Click the **Refresh** button to update the list.

- Delete:** Deletes the selected SMS message.
- Reply:** Opens a Create Message window to reply to the selected SMS message.
- Forward:** Opens a Create Message windows to forward the selected SMS message to another recipient.
- Refresh:** Click this button to check for new messages.



## Create Message

This page allows you to send an SMS to your contacts. Just fill in the phone number of the recipient, and type the content of the message. Then click the “Send Message” button to send out the message. If you would like to add more than one recipient, you must put a semicolon (;) between each of the phone numbers.

**Receiver:** Type the phone number of the recipient.

**Text Message:** Type the message that you would like to send.

**Send Message:** Click this button to send the message.

**Cancel:** Click this button to clear the message.

The screenshot shows a 'CREATE MESSAGE' dialog box. It has two input fields: 'Receiver:' and 'Text message:'. Below the 'Text message:' field is a note: 'Add '+' for international format of the phone number.' At the bottom, there are status messages: 'Current input text length : 0.' and 'The max. length of a message is 160 characters for pure alphabetical or numeric.' There are also 'Send message' and 'Cancel' buttons at the bottom right.

# Advanced

The **ADVANCED** pages allow you to configure the more advanced settings of the router, such as Virtual Server, MAC and URL filtering, and advanced wireless and network settings. To view the advanced configuration pages, click on **ADVANCED** at the top of the screen.



## Virtual Server

The device can be configured as a virtual server so that users can access services such as Web or FTP via the public (WAN) IP address of the router. You can also allow the settings to run on a specified schedule. After modifying any settings, click **Save Settings** to save your changes.

**Well-known Services:** This contains a list of pre-defined services. You can select a service, select a rule ID, then click the **Copy to** button to copy the default settings for that service to the specified rule ID.

**ID:** Specifies which rule to copy the selected **Well known service** settings to when you click the **Copy to** button.

**Use schedule rule:** Select a schedule to use and copy to the specified rule ID when you click the **Copy to** button. You may select **Always On** or use a specific schedule that you have defined. To create and edit schedules, please refer to "Schedules" on page 58.

**D-Link**

**DWR-921 //**

**SETUP**   **ADVANCED** (highlighted)   **TOOLS**   **STATUS**   **SUPPORT**

**VIRTUAL SERVER**

The Virtual Server option allows you to define a single public port on your router for redirection to an internal LAN IP Address and Private LAN port if required. This feature is useful for hosting online services such as FTP or Web Servers.

**Well known services**: -- select one -- **Copy to** ID: -- **Use schedule rule**: **ALWAYS ON**

**VIRTUAL SERVERS LIST**

ID	Service Ports	Server IP : Port	Enable	Schedule Rule#
1			<input type="checkbox"/>	<b>Add New Rule...</b>
2			<input type="checkbox"/>	<b>Add New Rule...</b>
3			<input type="checkbox"/>	<b>Add New Rule...</b>
4			<input type="checkbox"/>	<b>Add New Rule...</b>

**Helpful Hints...**

- You can select your computer from the list of DHCP clients in the Computer Name drop down menu, or enter the IP address of the computer you would like to open the specified port to.
- This feature allows you to open a range of ports to a computer on your network. To do so, enter the first port in the range that you would like to open in the first box under Public Port and last port of the range in the second box. Note that you enter the first port in the range that the internal port used in the first box under Internal Port and the last port in the second.
- To open a single port using this feature, simply enter the same number in both boxes.

**More...**

**VIRTUAL SERVERS LIST**

**ID:** This identifies the rule.

**Service Ports** Enter the public port(s) you want to open.

**Server IP: Port:** Enter the IP address and port of the computer on your local network that you want to forward the Service Ports to.

**Enable:** Check the box to enable the specified rule.

**Schedule Rule #:** Specify the schedule rule number. To create schedules, click on the **Add New Rule** button. For further information on schedules, please refer to "Schedules" on page 58.

**VIRTUAL SERVERS LIST**

ID	Service Ports	Server IP : Port	Enable	Schedule Rule#
1	5001	192.168.0.50 : 5001	<input checked="" type="checkbox"/>	<b>Add New Rule...</b>
2			<input type="checkbox"/>	<b>Add New Rule...</b>
3			<input type="checkbox"/>	<b>Add New Rule...</b>
4			<input type="checkbox"/>	<b>Add New Rule...</b>
5			<input type="checkbox"/>	<b>Add New Rule...</b>
6			<input type="checkbox"/>	<b>Add New Rule...</b>
7			<input type="checkbox"/>	<b>Add New Rule...</b>
8			<input type="checkbox"/>	<b>Add New Rule...</b>

# Application Rules

Some applications require multiple connections, such as Internet gaming, video conferencing, and Internet telephony. These applications may have difficulty working through NAT (Network Address Translation). **Application Rules** allow some of these applications to work with the DWR-921 by opening ports after detecting traffic being sent through a trigger port. After modifying any settings, click **Save Settings** to save your changes.

**Popular Applications:** Select from a list of popular applications. You can select a service, select a rule ID, then click the **Copy to** button to copy the default settings for that service to the specified rule ID.

**ID:** Specifies which rule to copy the selected **Popular application** settings to when you click the **Copy to** button.

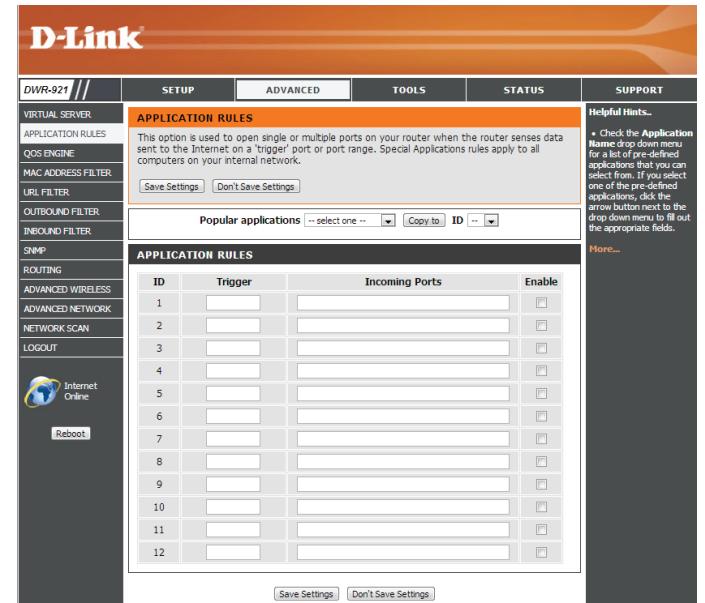
## APPLICATION RULES

**ID:** This identifies the rule.

**Trigger:** Enter the port to listen to in order to trigger the rule.

**Incoming Ports:** Specify the incoming port(s) to open when traffic comes over the **Trigger** port.

**Enable:** Check the box to enable the specified rule.



# QoS Engine

The **QoS Engine** improves your online gaming or streaming media experience by ensuring that your game or media traffic is prioritized over other network traffic, such as FTP or web. For best performance, use the Automatic Classification option to automatically set the priority for your applications. After modifying any settings, click **Save Settings** to save your changes.

## QOS ENGINE SETUP

**Enable QoS Packet Filter:** Select this box to enable the QoS feature.

**Upstream Bandwidth:** Specify the maximum upstream bandwidth here (e.g. 400 Kbps).

**Use Schedule Rule:** Select a schedule to use and copy to the specified rule ID when you click the **Copy to** button. You may select **Always On** or use a specific schedule that you have defined. To create and edit schedules, please refer to "Schedules" on page 58.

## QOS RULES

**ID:** This identifies the rule.

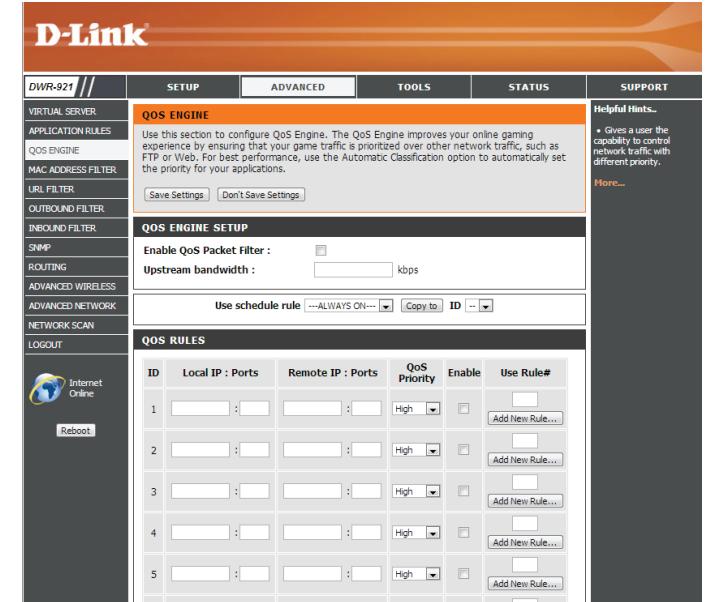
**Local IP : Ports:** Specify the local IP address(es) and port(s) for the rule to affect.

**Remote IP : Ports:** Specify the remote IP address(es) and port(s) for the rule to affect.

**QoS Priority:** Select what priority level to use for traffic affected by the rule: **Low, Normal, or High.**

**Enable:** Check the box to enable the specified rule.

**Use Rule #:** Specify the schedule rule number. To create a new schedule, click on the **Add New Rule** button. For more information about schedules, please refer to "Schedules" on page 58.



# MAC Address Filter

The **MAC (Media Access Controller) Address Filter** option is used to control network access based on the MAC address of the network adapter. A MAC address is a unique ID assigned by the manufacturer of the network adapter. This feature can be configured to ALLOW or DENY network/Internet access. After modifying any settings, click **Save Settings** to save your changes.

## MAC FILTERING SETTINGS

**MAC Address Control:** Tick this box to enable MAC Filtering.

**Connection Control:** Check the box to allow wireless and wired clients with **C** selected to connect to this device. You can also select to **allow** or **deny** connections from unspecified MAC addresses.

**Association Control:** Check the box to allow wireless clients with **A** selected can associate to the wireless LAN. You can also select to **allow** or **deny** connections from unspecified MAC addresses.

## MAC FILTERING RULES

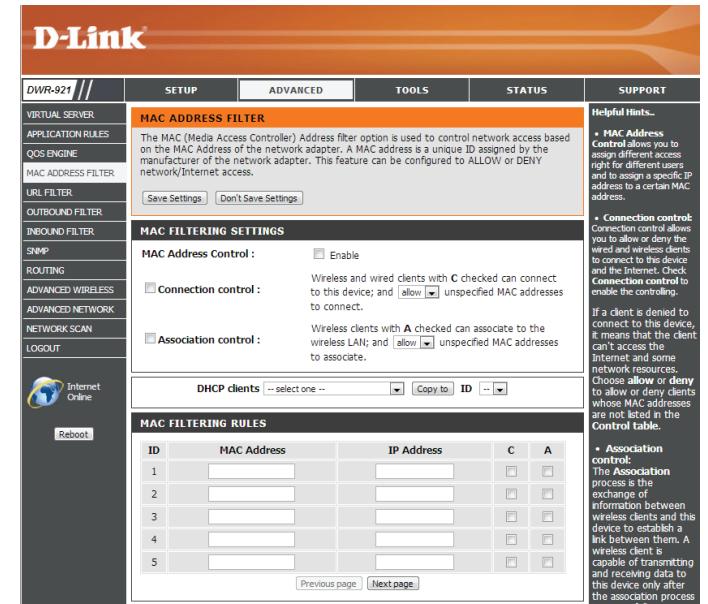
**ID:** This identifies the rule.

**MAC Address:** Specify the MAC address of the computer to be filtered.

**IP Address:** Specify the last section of the IP address.

**C:** If this box is ticked, the rule will follow the connection control setting specified in MAC filtering settings specified above.

**A:** If this box is ticked, the rule will follow the association control setting specified in MAC filtering settings specified above.



# URL Filter

**URL Filter** allows you to set up a list of websites that will be blocked from users on your network. After modifying any settings, click **Save Settings** to save your changes.

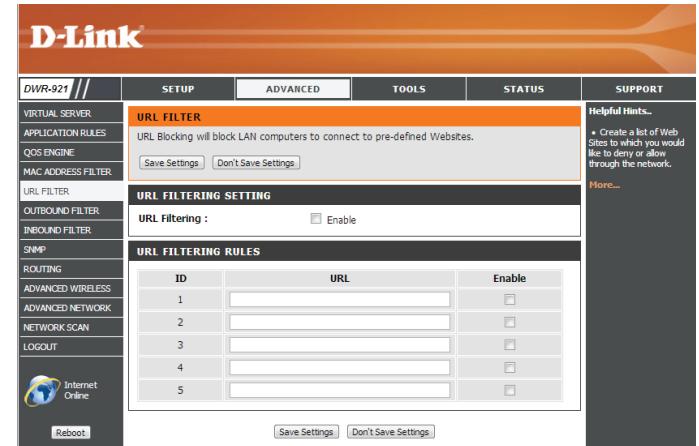
**URL Filtering:** Check the box to enable URL Filtering.

## URL FILTERING RULES

**ID:** This identifies the rule.

**URL:** Enter URL that you would like to block. All URLs that begin with this URL will be blocked.

**Enable:** Check the box to enable the specified rule.



# Outbound Filter

**Outbound Filter** enables you to control what packets are allowed to be sent out to the Internet. The outbound filter applies to all outbound packets. After modifying any settings, click **Save Settings** to save your changes.

## OUTBOUND FILTER SETTING

**Outbound Filter:** Select this box to **Enable** outbound filtering.

**Use Schedule Rule:** Select a schedule to use and copy to the specified rule ID when you click the **Copy to** button. You may select **Always On** or use a specific schedule that you have defined. To create and edit schedules, please refer to "Schedules" on page 58.

## OUTBOUND FILTER RULES LIST

Here, you can select whether to **Allow** or **Deny** all outgoing traffic except for traffic that matches the listed rules.

**ID:** This identifies the rule.

**Source IP : Ports:** Specify the local IP address and then specify the port after the colon.

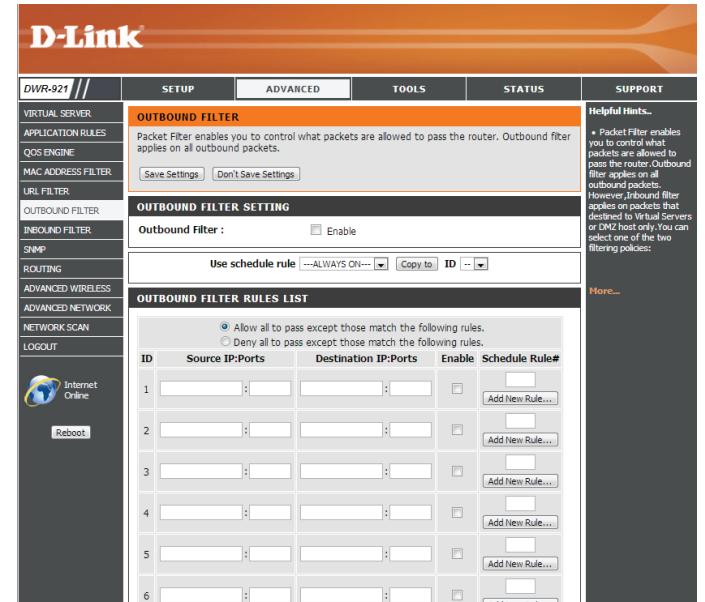
**Destination IP : Ports:** Specify the remote IP address and then the port after the colon.

**Enable:** Check the box to enable the specified rule.

**Schedule Rule #:** Specify the schedule rule number. Click on the **Add New Rule** button to create a new schedule rule.

**Previous Page:** Go back to the previous filter page.

**Next Page:** Advance to the next filter page.



# Inbound Filter

**Inbound Filter** enables you to control what packets are allowed to come in to your network from the Internet. The inbound filter only applies to packets that are destined for Virtual Servers or DMZ hosts. After modifying any settings, click **Save Settings** to save your changes.

## INBOUND FILTER SETTING

**Inbound Filter:** Select this box to **Enable** the filter.

**Use Schedule Rule:** Select a schedule to use and copy to the specified rule ID when you click the **Copy to** button. You may select **Always On** or use a specific schedule that you have defined. To create and edit schedules, please refer to "Schedules" on page 58.

## INBOUND FILTER RULES LIST

Here, you can select whether to **Allow** or **Deny** all incoming traffic except for traffic that matches the listed rules.

**ID:** This identifies the rule.

**Source IP : Ports:** Specify the local IP address and then specify the port after the colon.

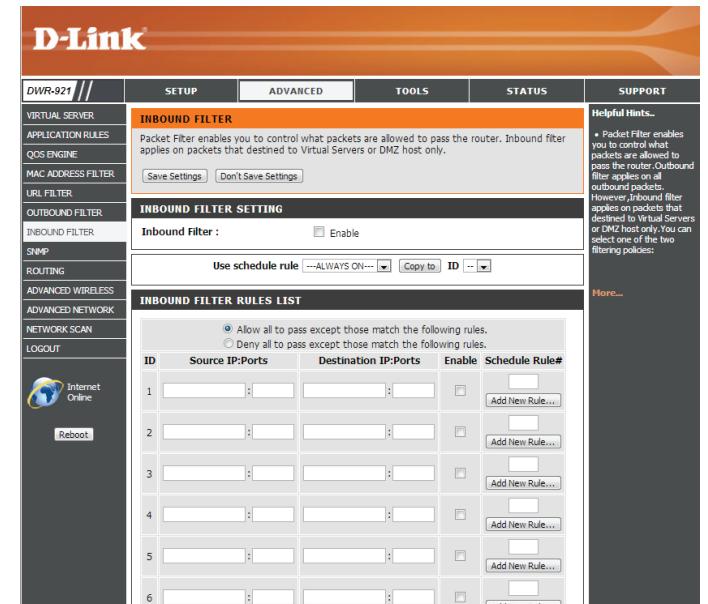
**Destination IP : Ports:** Specify the remote IP address and then the port after the colon.

**Enable:** Check the box to enable the specified rule.

**Schedule Rule #:** Specify the schedule rule number. Click on the **Add New Rule** button to create a new schedule rule.

**Previous Page:** Go back to the previous filter page.

**Next Page:** Advance to the next filter page.



# SNMP

**SNMP** (Simple Network Management Protocol) is a widely used network monitoring and control protocol that reports activity on each network device to the administrator of the network. SNMP can be used to monitor traffic and statistics of the DWR-921. The DWR-921 supports SNMP v1 and v2c. After modifying any settings, click **Save Settings** to save your changes.

## SNMP

**SNMP Local:** Select whether to **Enable or Disable** local SNMP administration.

**SNMP Remote:** Select whether to **Enable or Disable** remote SNMP administration.

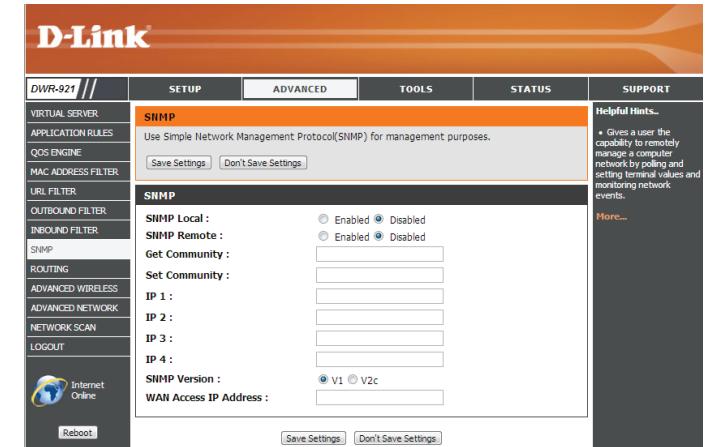
**Get Community:** Enter the password **public** in this field to allow read-only access to network administration using SNMP. You can view the network, but no configuration is possible with this setting.

**Set Community:** Enter the password **private** in this field to enable read/write access to the network using SNMP.

**IP 1/IP 2/IP 3/IP 4:** Enter up to 4 IP addresses to use as trap targets for your network.

**SNMP Version:** Select the SNMP version of your system.

**WAN Access IP Address** If you want to limit remote access SNMP access, enter the IP address of the remote computer you will use to access this device; all other IP addresses will be denied remote SNMP access.



# Routing

The **Routing** page allows you to specify custom routes that determine how data is moved around your network. After modifying any settings, click **Save Settings** to save your changes.

## RIP SETTING

**RIP:** Check the box to enable routing, then select which routing protocol to use:

- **RIPv1:** Protocol in which the IP address is routed through the internet.
- **RIPv2:** Enhanced version of RIPv1 with added features such as authentication, routing domain, next hop forwarding, and subnet-mask exchange.

## ROUTING RULES

**ID:** This identifies the rule.

**Destination:** Enter in the IP of the specified network that you want to access using the static route.

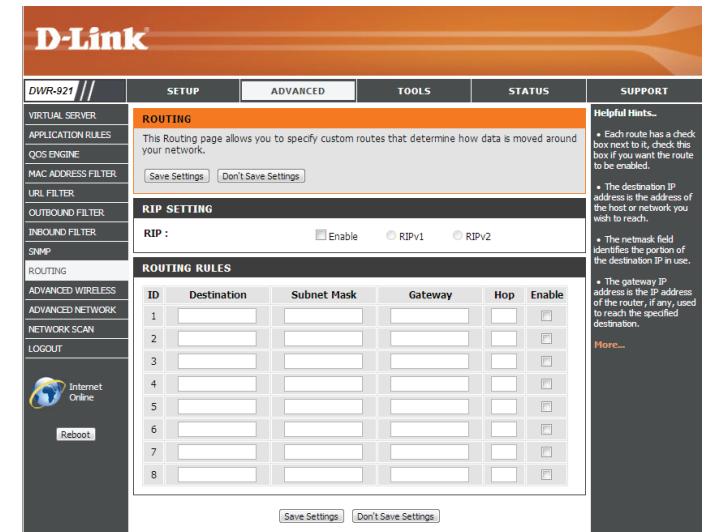
**Subnet Mask:** Enter in the subnet mask to be used for the specified network.

**Gateway:** Enter in the gateway IP address for the specified network.

**Hop:** Enter in the amount of hops it will take to reach the specified network.

**Note:** In a transmission path, each link is terminated at a network device such as a router or gateway. The number of hops equals the number of routers or gateways that data must pass through before reaching the destination.

**Enable:** Select this box to enable the rule.



# Advanced Wireless

**Advanced Wireless** contains settings which can negatively affect the performance of your router if configured improperly. Do not change these settings unless you are already familiar with them or have been instructed to make the change by one of our support personnel. After modifying any settings, click **Save Settings** to save your changes.

**Beacon Interval:** Specify a value for the beacon interval. Beacons are packets sent by an access point to synchronize a wireless network. 100 is the default setting and is recommended.

**Transmit Power:** Set the transmit power of the antennas.

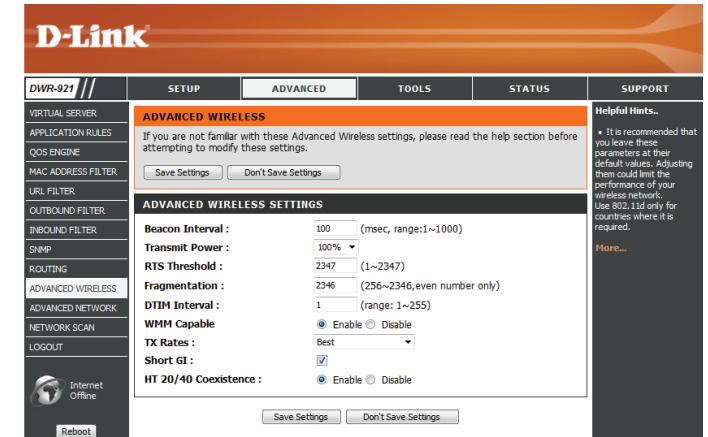
**RTS Threshold:** This value should remain at its default setting of 2347. If inconsistent data flow is a problem, only a minor modification should be made.

**Fragmentation:** The fragmentation threshold, which is specified in bytes, determines whether packets will be fragmented. Packets exceeding the 2346 byte setting will be fragmented before transmission. 2346 is the default setting.

**DTIM Interval:** Set the interval for DTIM. A Delivery Traffic Indication Message (DTIM) is a countdown informing clients of the next window for listening to broadcast and multicast messages. The default interval is 3.

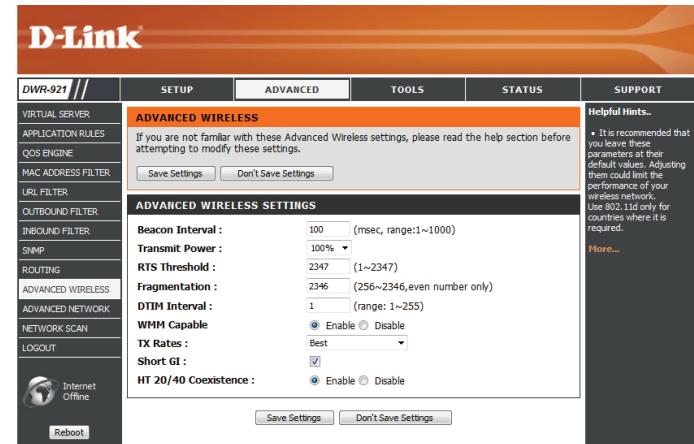
**WMM Capable:** WMM (Wi-Fi Multimedia) is a QoS (Quality of Service) system for your wireless network. Enable this option to improve the quality of video and voice applications for your wireless clients.

**TX Rates:** Select the basic transfer rates based on the speed of wireless adapters on your wireless network. It is strongly recommended to keep this setting to **Auto**.



**Short GI:** Check this box to reduce the guard interval to 400 ns. This can increase the throughput rate provided that the delay spread of the connection is also low. However, it can also increase error rate in some installations, due to increased sensitivity to radio-frequency reflections. Select the option that works best for your installation.

**HT 20/40 Coexistence:** Enable this option to reduce interference from other wireless networks in your area. If the channel width is operating at 40 MHz and there is another wireless network's channel over-lapping and causing interference, the router will automatically change to 20 MHz.

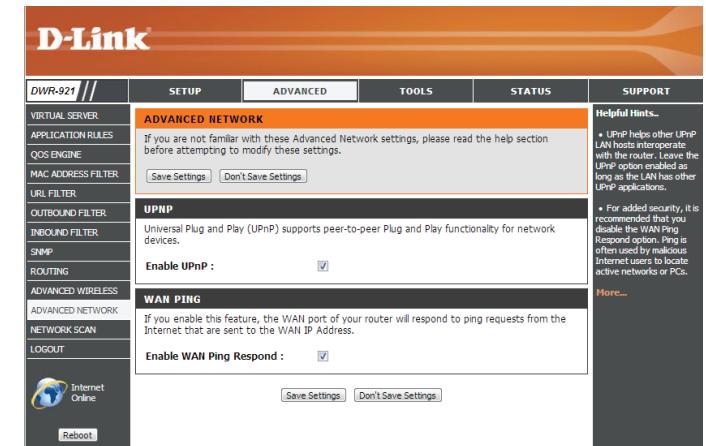


# Advanced Network

**Advanced Network** contains settings which can change the way the router handles certain types of traffic. We recommend that you do not change any of these settings unless you are already familiar with them or have been instructed to make the change by one of our support personnel. After modifying any settings, click **Save Settings** to save your changes.

**Enable UPnP:** Check the box to enable the Universal Plug and Play (UPnP™) feature. UPNP provides compatibility with various networking equipment, software, and peripherals.

**Enable WAN Ping Respond:** Select the box to allow the WAN port to be “pinged.” Blocking WAN pings may provide some extra security from hackers.

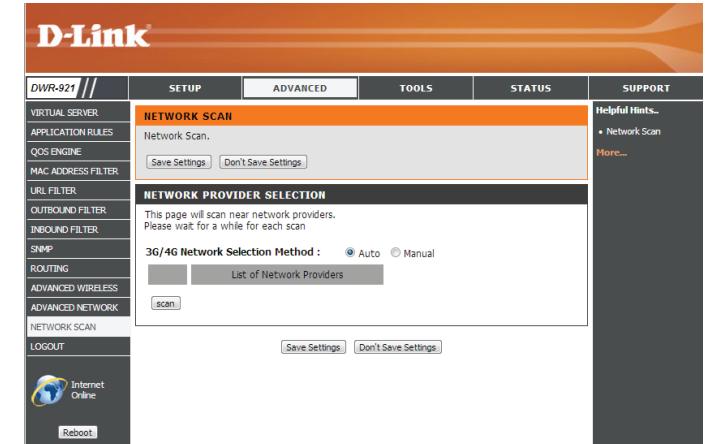


# Network Scan

This page lets you set whether to allow the DWR-921 to automatically select a 3G/4G network based on the inserted SIM card, and allows you to manually scan for networks and select one to connect to.

- 3G/4G Network Selection Method:** Leave this setting on **Auto** to allow the DWR-921 to automatically select a cellular network to connect to. If you need to select a network manually, select **Manual**, click the **Scan** button, then select an available network to connect to.

**Note:** You will only be able to scan for networks if the DWR-921 is not currently connected to a 3G/4G network.



# Tools

The **TOOLS** pages allow you to adjust various system settings for your router, such as the system time, firmware, and custom schedules. To view the Tools pages, click on **TOOLS** at the top of the screen.



## Admin

The **Admin** page allows you to change the Administrator password and enable Remote Management. The admin has read/write access while users only have read-only access. Only the admin has the ability to change both admin and user account passwords. After modifying any settings, click **Save Settings** to save your changes.

### ADMINISTRATOR

**Admin Password:** Enter and confirm the password that the admin account will use to access the router's management interface.

### REMOTE MANAGEMENT

**Remote Management:** Tick this check box to enable remote management. Remote management allows the DWR-921 to be configured over the Internet through a web browser. A username and password will still be required to access the web-management interface.

**IP Allowed to Access:** Enter the Internet IP address of the PC that has access to the broadband router. If you enter an asterisk (\*) in this field, then anyone will be able to access the router. Adding an asterisk (\*) into this field could present a security risk and is not recommended.

**Port:** This is the port number used to access the router. 8080 is the port usually used for the web-management interface.

D-Link

**ADMINISTRATOR SETTINGS**

To help secure your network, we recommend that you should choose a new password.

New Password :   
Confirm Password :

**REMOTE MANAGEMENT**

Enable Remote Management :  Enabled  
IP Allowed to Access :  0.0.0  
Port :  8080

Helpful Hints...

- \* For security reasons, it is recommended that you change the password for the admin and user accounts. Be sure to write down the new and password to avoid having to reset the router in case they are forgotten.
- \* Enabling Remote Management, allows you or others to change the router configuration from a computer on the Internet.
- \* Choose a port to open for remote management.

More...

# Time

This section will help you set the time zone that you are in and an NTP (Network Time Protocol) server to use. Daylight Saving can also be configured to adjust the time when needed. After modifying any settings, click **Save Settings** to save your changes.

## TIME AND DATE CONFIGURATION

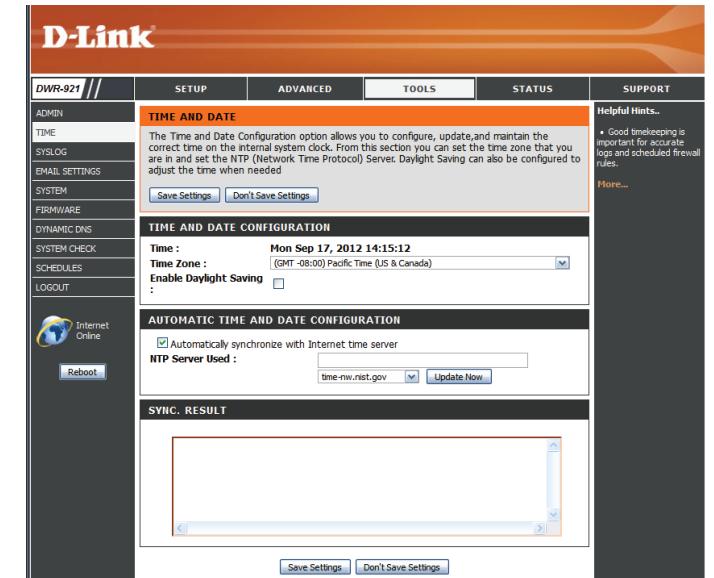
**Time Zone:** Select the appropriate **Time Zone** from the drop-down box.

**Enable Daylight Saving:** Check the box to allow for daylight saving adjustments. Use the drop-down boxes to specify a start date and end date for daylight saving time adjustments.

## AUTOMATIC TIME AND DATE CONFIGURATION

Check the **Automatically synchronize with Internet time server** box to allow the router to use an NTP server to update the router's internal clock.

**NTP Server Used:** Enter an NTP server to use for time synchronization, or use the drop-down box to select one. Click the **Update Now** button to synchronize the time with the NTP server.

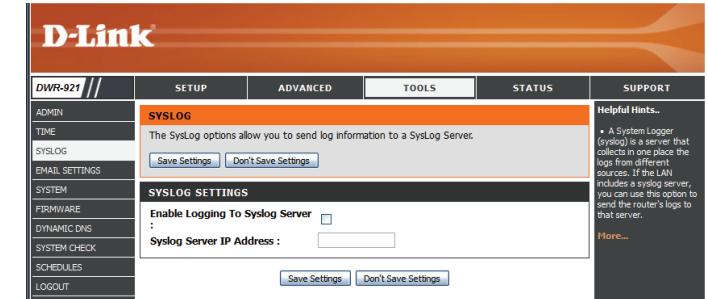


# Syslog

The DWR-921 keeps a running log of events and activities occurring on the router. You may send these logs to a Syslog server on your network. After modifying any settings, click **Save Settings** to save your changes.

**Enable Logging to Syslog Server:** Check the box to send the router logs to a Syslog server.

**Syslog Server IP Address:** Enter the IP address of the Syslog server that the router will send the logs to.



# Email Settings

**Email Settings** allow you to send the system log files, router alert messages, and firmware update notifications to an email address. After modifying any settings, click **Save Settings** to save your changes.

**Enable Email Notification:** When this option is enabled, router activity logs will be emailed to the specified email address.

**SMTP Server IP and Port:** Enter the SMTP server IP address the router will use to send emails. Enter the complete IP address followed by a colon(:) and the port number. (e.g. 123.123.123.1:25).

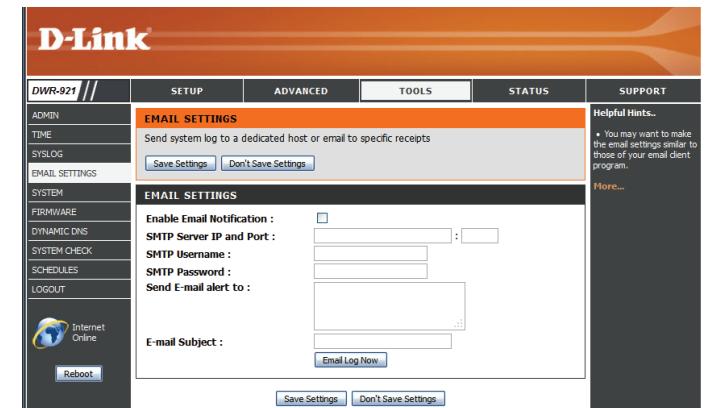
**SMTP Username:** Enter the username for the SMTP account.

**SMTP Password:** Enter the password for the SMTP account.

**Send Email Alert to:** Enter the email address where you would like the router to send emails to.

**Email Subject:** Enter a subject for the email.

**Email Log Now:** Click this button to send the current logs to the specified email address.



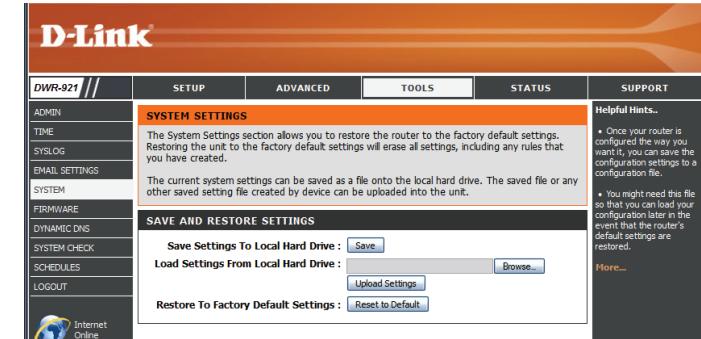
# System

Here, you can save the current system settings to a local hard drive. After modifying any settings, click **Save Settings** to save your changes.

**Save Settings To Local Hard Drive:** Use this option to save your current router configuration settings to a file. Click **Save** to open a file dialog, and then select a location and file name for the settings.

**Load Settings From Local Hard Drive:** Use this option to load previously saved router configuration settings. Click **Browse...** and select the saved file and then click the **Upload Settings** button to upload the settings to the router.

**Restore To Factory Default Settings:** This option will restore all settings back to their defaults. Any settings that have not been backed up will be lost, including any rules that you have created.



# Firmware

Here, you can upgrade the firmware of your router. Make sure the firmware you want to use is on the local hard drive of the computer and then click **Browse** to upload the file. You can check for and download firmware updates at the D-Link support site at <http://support.dlink.com>. After modifying any settings, click **Save Settings** to save your changes.

**Current Firmware Version:** Displays your current firmware's version.

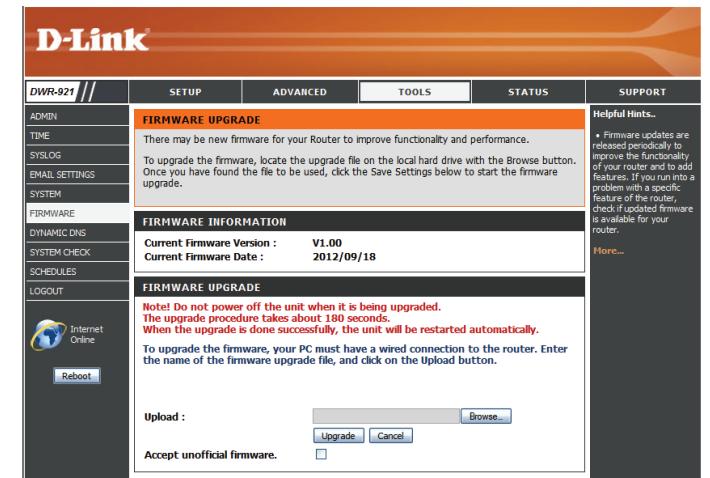
**Current Firmware Date:** Displays your current firmware's release date.

**Upload:** After you have downloaded a new firmware, click **Browse** to locate the firmware on your computer, then click **Upload** to start the firmware upgrade.

**Warning:** You must use a wired connection to upload the firmware file; do not use a wireless connection. During the upgrade process, do not power off your computer or router, and do not refresh the browser window until the upgrade is complete.

**Accept Unofficial Firmware:** If the firmware you want to install is not an official D-Link release, you will need to check this box.

**Warning:** Unofficial firmware is not supported, and may cause damage to your device. Use of unofficial firmware is at your own risk.



# Dynamic DNS

The DDNS feature allows you to host a server (Web, FTP, or Game Server) using a domain name that you have purchased (such as [www.exampledomain.com](http://www.exampledomain.com)) with your dynamically assigned IP address. You can use one of the listed DDNS service, or you can sign up for D-Link's free DDNS service at [www.dlinkddns.com](http://www.dlinkddns.com). After modifying any settings, click **Save Settings** to save your changes.

**DDNS:** Tick this checkbox to enable the DDNS feature.

**Provider:** Select a DDNS service provider to use.

**Host Name:** Enter the **Host Name** that you registered with your DDNS service provider.

**Username / E-mail:** Enter the **Username** for your DDNS account.

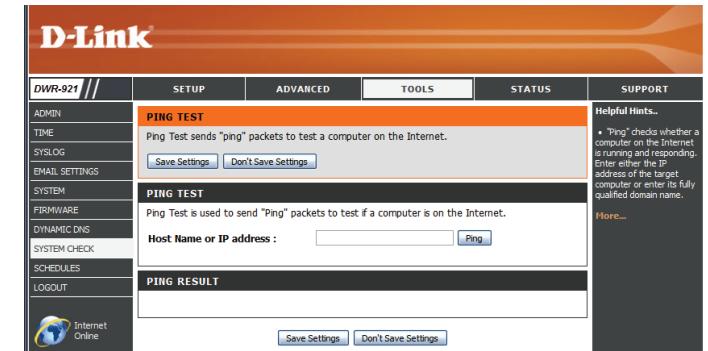
**Password / Key:** Enter the **Password** for your DDNS account.



# System Check

This useful diagnostic utility can be used to check if a computer is connected to the network. It sends ping packets and listens for responses from the specific host. After modifying any settings, click **Save Settings** to save your changes.

**Host Name or IP Address:** Enter a host name or the IP address that you want to ping and click the **Ping** button. The results of the ping attempt will be displayed in the **PING RESULT** section below.



# Schedules

This section allows you to manage schedule rules for various firewall and parental control features. After modifying any settings, click **Save Settings** to save your changes.

**Enable Schedule:** Check this box to enable schedules.

**Edit:** Click this icon to edit the selected rule. (see below)

**Delete:** Click this icon to delete the selected rule.

**Previous Page:** Click this button to go to the previous page of rules.

**Next Page:** Click this button to go to the next page of rules.

Click this button to specify the start time, end time, and name of the rule.

**Add New Rule..:** Click this button to create a new rule. (see below)

**Name of Rule #:** Enter a name for your new schedule.

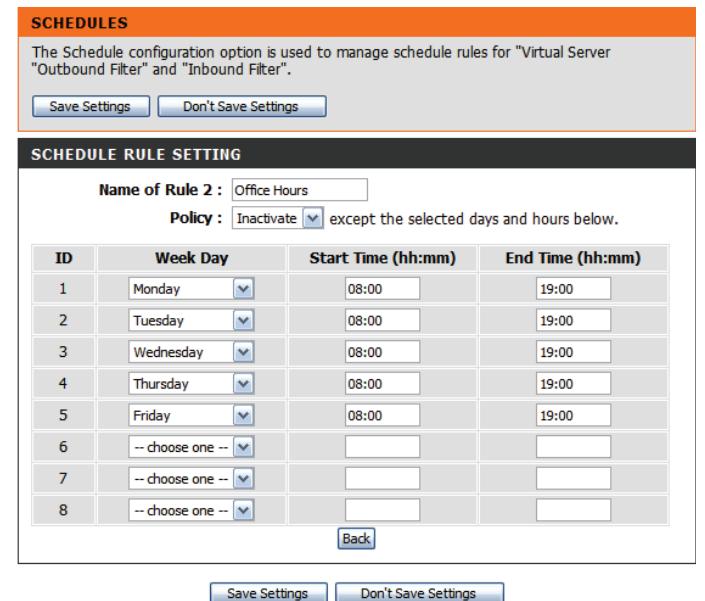
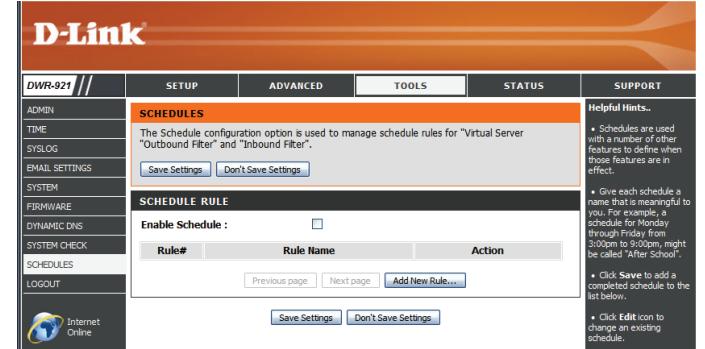
**Policy:** Select Activate or Inactivate to decide whether features that use the schedule should be active or inactive except during the times specified.

**Week Day:** Select a day of the week for the start time and end time.

**Start Time (hh:mm):** Enter the time at which you would like the schedule to become active.

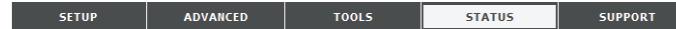
**End Time (hh:mm):** Select the time at which you would like the schedule to become inactive.

After making your changes, click **Save Settings** to save the schedule.



# Status

The **STATUS** pages allow you to see the current status of the router for various categories, including WAN, 3G, network, and wireless. To view the Status pages, click on **STATUS** at the top of the screen.



## Device Info

All of your Internet and network connection details are displayed on this page. The firmware version is also displayed here.

- General:** Displays the current time and firmware version.
- WAN:** Displays the WAN connection details of the router.
- 3G Card:** Displays the 3G connection details of the router.
- LAN:** Displays the LAN connection details of the router.
- Wireless LAN:** Displays the wireless LAN connection details of the router
- LAN Computers:** Displays the list of clients connected to the router.

**DEVICE INFORMATION**  
All of your Internet and network connection details are displayed on this page. The firmware version is also displayed here.  
[Refresh](#)

**GENERAL**  
Time : Sun Sep 16, 2012 22:16:11 -0800  
Firmware Version : V1.00 , 2012/09/04

**WAN**  
Connection Type : DHCP Client  
Network Status : Established  
Remaining Lease Time : 6 Hour 2 Min 5 Sec  
[Renew](#) [Release](#)  
MAC Address : 84:C9:82:E2:FC:7F  
IP Address : 172.17.5.131  
Subnet Mask : 255.255.255.0  
Default Gateway : 192.168.168.249 , 192.168.168.201  
DNS Server : 192.168.168.249 , 192.168.168.201

**3G/4G CARD**  
Card Info : N/A  
Link Status : Connecting...  
Network Name : N/A

**LAN**  
MAC Address : 84:C9:82:E2:FC:7F  
IP Address : 192.168.0.1  
Subnet Mask : 255.255.255.0  
DHCP Server : Enabled

**WIRELESS LAN**  
MAC Address : 84:C9:82:E2:FC:7F  
Wireless : Enabled  
SSID : dlink\_DWR-921  
Security : Auto(None)  
Channel : 11  
802.11 Mode : B/G/N Mixed

**LAN COMPUTERS**

IP Address	Name	MAC
192.168.0.50	06955pcwinxp	00-19-B9-43-71-1E

# Log

Here, you can view and download the system log.

**Previous:** Click this button to go to the previous page of the log.

**Next:** Click this button to go to the next page of the log.

**First Page:** Click this button to skip to the first page of the log.

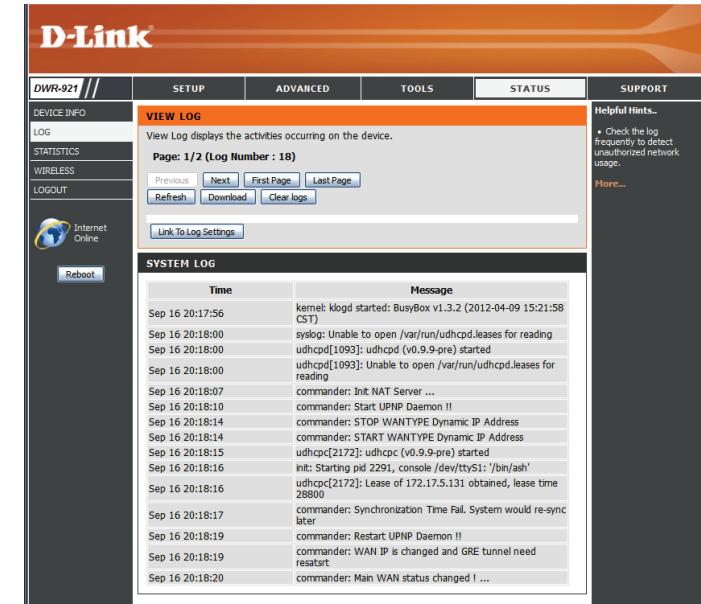
**Last Page:** Click this button to skip to the last page of the log.

**Refresh:** Click this button to refresh the system log.

**Download:** Click this button to download the current system log to your computer.

**Clear Logs:** Click this button to clear the system log.

**Link To Log Settings:** Click this button for a link that goes to the Log Settings page.



# Statistics

Here you can view the packets transmitted and received by your router for both the WAN and LAN ports. The traffic counter will reset if the device is rebooted. Click the Refresh button to refresh the WAN statistics.

The screenshot shows the 'STATISTICS' page of the D-Link DWR-921 router's web interface. The top navigation bar includes links for SETUP, ADVANCED, TOOLS, STATUS (which is selected), and SUPPORT. The left sidebar has links for DEVICE INFO, LOG, STATISTICS (selected), WIRELESS, and LOGOUT, along with an 'Internet Online' status indicator and a 'Reboot' button. The main content area is divided into two sections: 'TRAFFIC STATISTICS' and 'WAN STATISTICS INFORMATION'. The 'TRAFFIC STATISTICS' section contains a brief description and a 'Refresh' button. The 'WAN STATISTICS INFORMATION' section displays a table with three columns: Statistics, Inbound, and Outbound. The table data is as follows:

Statistics	Inbound	Outbound
Octets	395173674	26541068
Unicast packets	381673	212624
Multicast packets	56653	0

To the right of the table is a 'Helpful Hints..' section with a bullet point explaining the traffic statistics summary and a 'More...' link.

# Wireless

This table displays a list of wireless clients that are connected to your wireless router. Click **Refresh** to refresh the list.

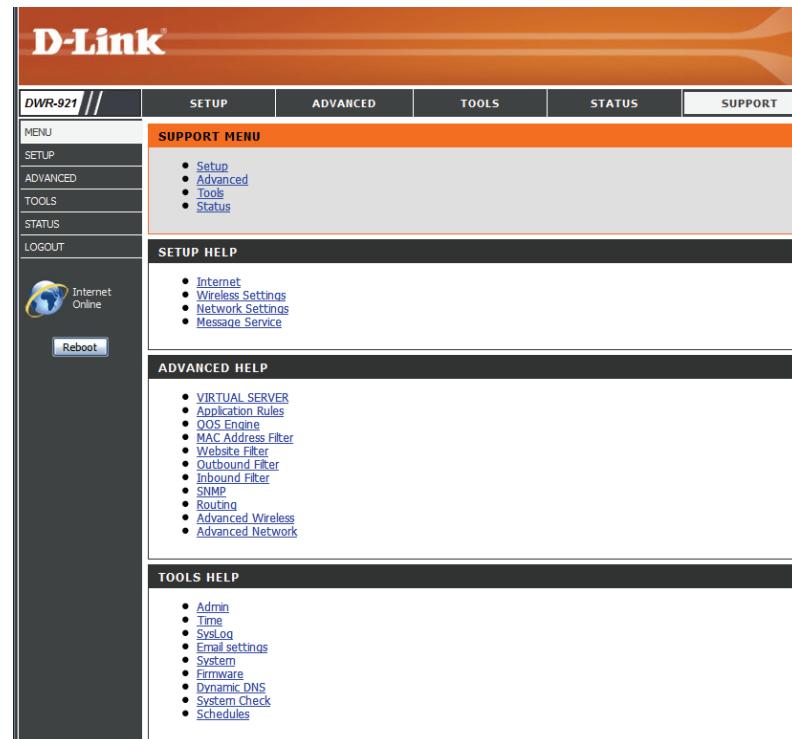
The screenshot shows the 'WIRELESS CLIENT LIST' section of the D-Link DWR-921 router's web interface. The left sidebar has links for DEVICE INFO, LOG, STATISTICS, WIRELESS (which is selected), and LOGOUT. The main area has tabs for SETUP, ADVANCED, TOOLS, STATUS (selected), and SUPPORT. The 'WIRELESS CLIENT LIST' section contains a message about viewing connected clients and a 'Refresh' button. The 'WIRELESS CLIENT TABLE' section shows one client entry:

ID	MAC Address
1	28-E0-2C-DC-0A-BE

The 'SUPPORT' sidebar includes 'Helpful Hints...' with a note about the list being current and a 'More...' link.

# Support

The **SUPPORT** pages provide help information for each section of the device's interface. To view the Support pages, click on **SUPPORT** at the top of the screen.



# Connecting to a Wireless Network Using Windows 7

Windows 7 users may use the built-in wireless utility to connect to a wireless network. If you are using another company's utility or Windows 2000, please refer to the user manual of your wireless adapter for help with connecting to a wireless network. Most utilities will have a "site survey" option similar to the Windows 7 utility as seen below.

If you receive the Wireless Networks Detected bubble, click on the center of the bubble to access the utility. You can also click on the wireless icon in your system tray (lower-right corner).

The utility will display any available wireless networks in your area.



Highlight the wireless network (SSID) you would like to connect to and click the **Connect** button.

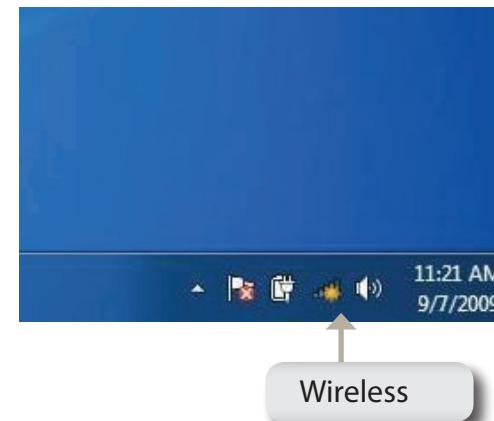
If you get a good signal but cannot access the Internet, check your TCP/IP settings for your wireless adapter. Refer to "Networking Basics" on page 80 for more information.



## Configuring Wireless Security

It is recommended to enable wireless security (WPA/WPA2) on your wireless router or access point before configuring your wireless adapter. If you are joining an existing network, you will need to know the security key or passphrase being used.

1. Click on the wireless icon in your system tray (lower-right corner).



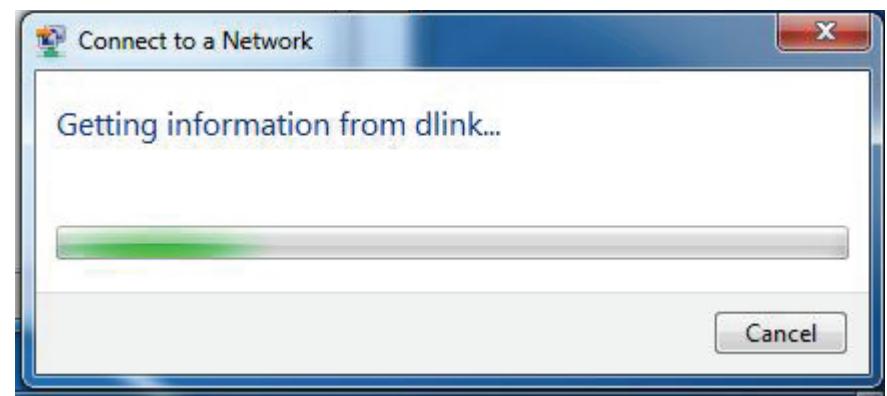
2. The utility will display any available wireless networks in your area.



3. Highlight the wireless network (SSID) you would like to connect to and click the **Connect** button.



4. The following window appears while your computer tries to connect to the router.



5. Enter the same security key or passphrase that is on your router and click **Connect**.

It may take 20-30 seconds to connect to the wireless network. If the connection fails, please verify that the security settings are correct. The key or passphrase must be exactly the same as on the wireless router.



# Using Windows Vista™

Windows® Vista™ users may use the built-in wireless utility. If you are using another company's utility or Windows® 2000, please refer to the user manual of your wireless adapter for help with connecting to a wireless network. Most utilities will have a "site survey" option similar to the Windows® Vista™ utility as seen below.

If you receive the **Wireless Networks Detected** bubble, click on the center of the bubble to access the utility.

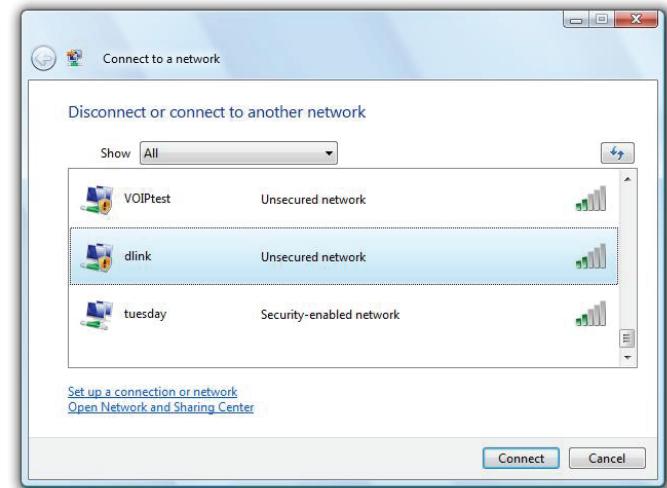
or

Right-click on the wireless computer icon in your system tray (lower-right corner next to the time). Select **Connect to a network**.



The utility will display any available wireless networks in your area. Click on a network (displayed using the SSID) and click the **Connect** button.

If you get a good signal but cannot access the Internet, check the TCP/IP settings for your wireless adapter. Refer to "Networking Basics" on page 80 for more information.



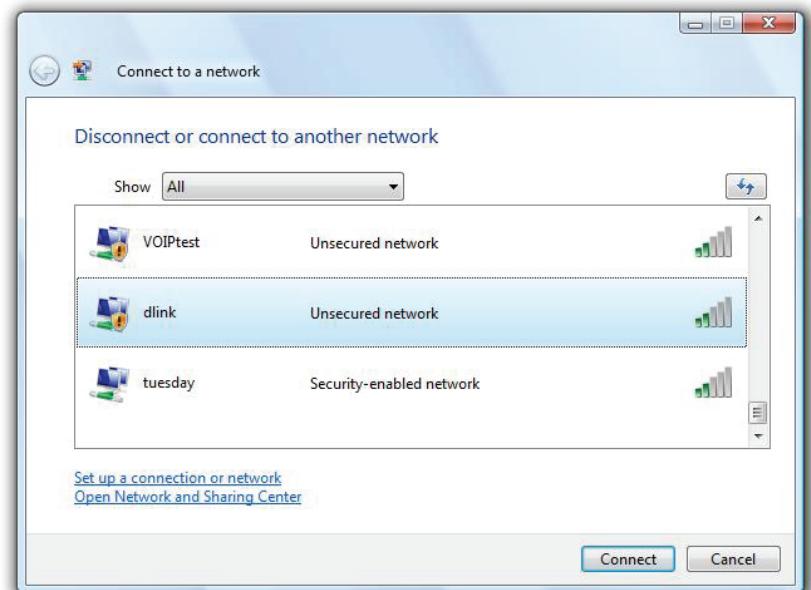
# Configuring Wireless Security

It is recommended to enable wireless security (WEP/WPA/WPA2) on your wireless router or access point before configuring your wireless adapter. If you are joining an existing network, you will need to know the security key or passphrase being used.

1. Open the Windows® Vista™ Wireless Utility by right-clicking on the wireless computer icon in your system tray (lower right corner of screen). Select **Connect to a network**.



2. Highlight the wireless network (SSID) you would like to connect to and click **Connect**.



3. Enter the same security key or passphrase that is on your router and click **Connect**.

It may take 20-30 seconds to connect to the wireless network. If the connection fails, please verify that the security settings are correct. The key or passphrase must be exactly the same as on the wireless router.



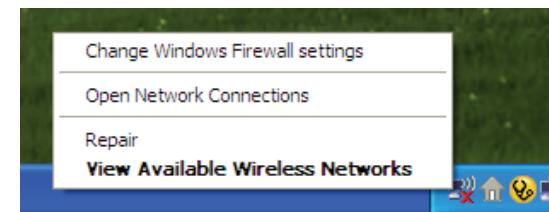
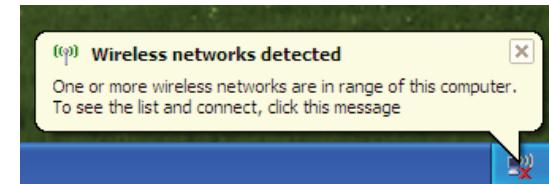
# Connect to a Wireless Network Using Windows® XP

Windows® XP users may use the built-in wireless utility (Zero Configuration Utility). The following instructions are for Service Pack 2 users. If you are using another company's utility or Windows® 2000, please refer to the user manual of your wireless adapter for help with connecting to a wireless network. Most utilities will have a "site survey" option similar to the Windows® XP utility as seen below.

If you receive the **Wireless Networks Detected** bubble, click on the center of the bubble to access the utility.

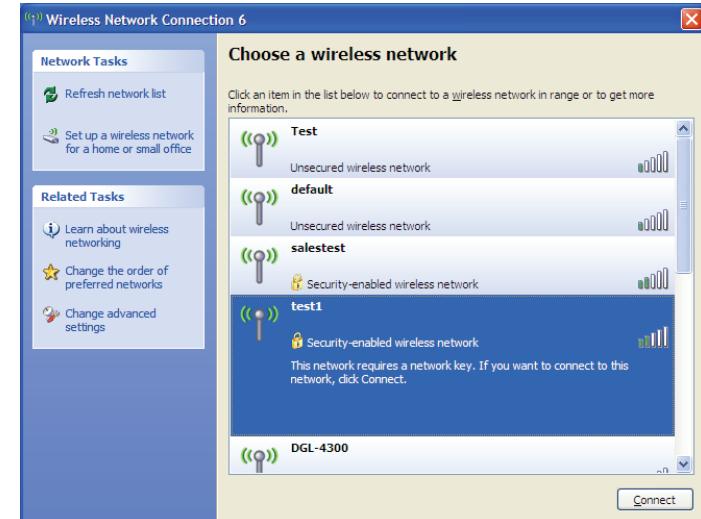
or

Right-click on the wireless computer icon in your system tray (lower-right corner next to the time). Select **View Available Wireless Networks**.



The utility will display any available wireless networks in your area. Click on a network (displayed using the SSID) and click the **Connect** button.

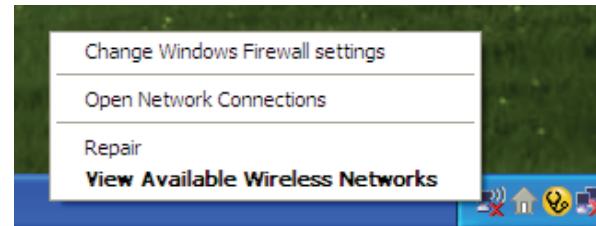
If you get a good signal but cannot access the Internet, check the TCP/IP settings for your wireless adapter. Refer to "Networking Basics" on page 80 for more information.



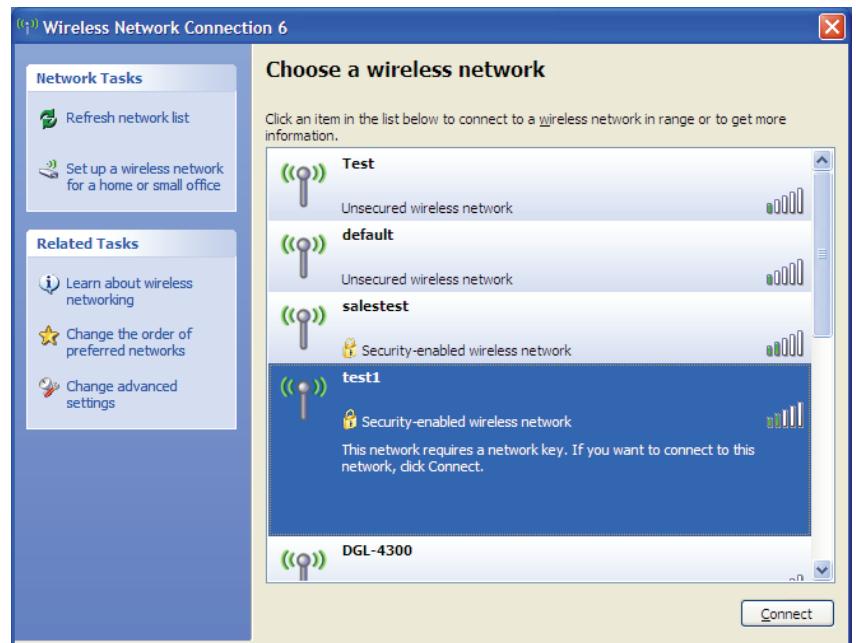
# Configure WEP

It is recommended to enable WEP on your wireless router or access point before configuring your wireless adapter. If you are joining an existing network, you will need to know the WEP key being used.

1. Open the Windows® XP Wireless Utility by right-clicking on the wireless computer icon in your system tray (lower-right corner of screen). Select **View Available Wireless Networks**.

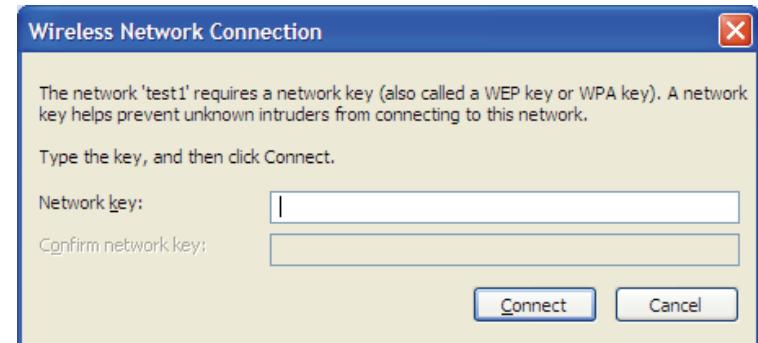


2. Highlight the wireless network (SSID) you would like to connect to and click **Connect**.



3. The **Wireless Network Connection** box will appear. Enter the same WEP key that is on your router and click **Connect**.

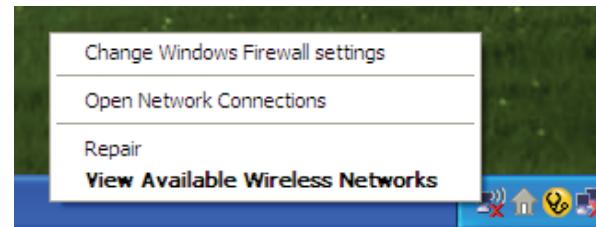
It may take 20-30 seconds to connect to the wireless network. If the connection fails, please verify that the WEP settings are correct. The WEP key must be exactly the same as on the wireless router.



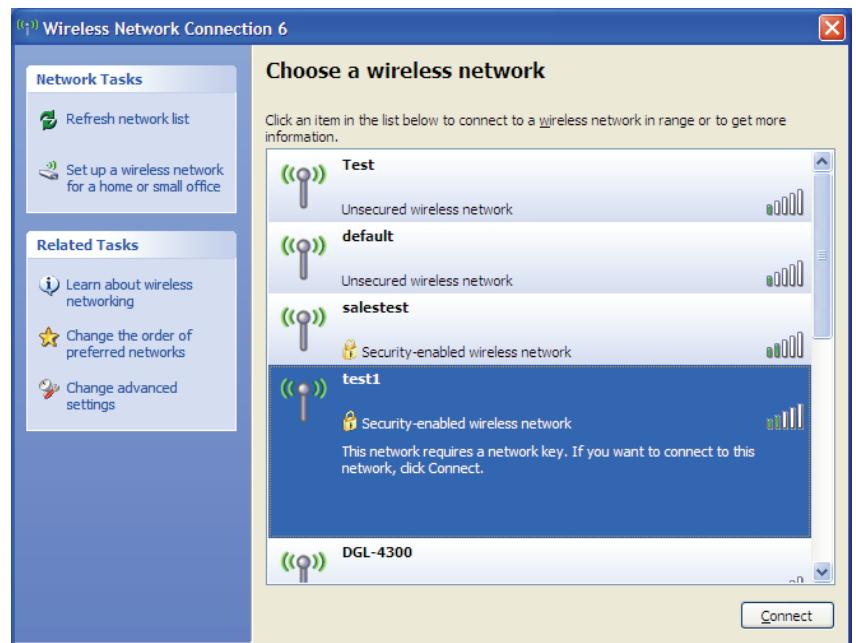
# Configure WPA-PSK

It is recommended to enable WPA on your wireless router or access point before configuring your wireless adapter. If you are joining an existing network, you will need to know the WPA key being used.

1. Open the Windows® XP Wireless Utility by right-clicking on the wireless computer icon in your system tray (lower-right corner of screen). Select **View Available Wireless Networks**.

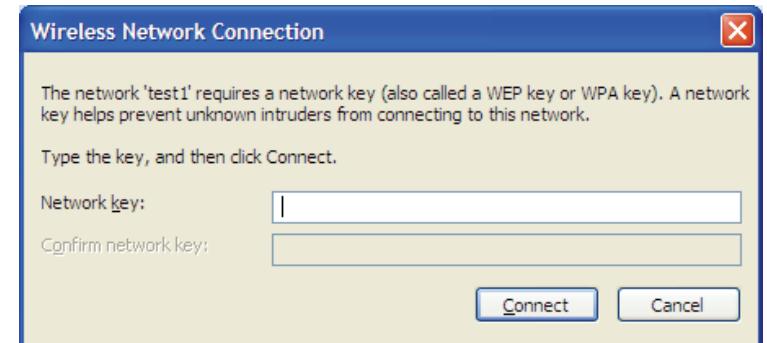


2. Highlight the wireless network (SSID) you would like to connect to and click **Connect**.



3. The **Wireless Network Connection** box will appear. Enter the WPA-PSK passphrase and click **Connect**.

It may take 20-30 seconds to connect to the wireless network. If the connection fails, please verify that the WPA-PSK settings are correct. The WPA-PSK passphrase must be exactly the same as on the wireless router.



# Troubleshooting

This chapter provides solutions to problems that can occur during the installation and operation of the DWR-921. Read the following descriptions if you are having problems.

## 1. Why can't I access the web-based configuration utility?

When entering the IP address of the D-Link router (192.168.0.1 for example), you are not connecting to a website on the Internet or have to be connected to the Internet. The device has the utility built-in to a ROM chip in the device itself. Your computer must be on the same IP subnet to connect to the web-based utility.

- Make sure you have an updated Java-enabled web browser. We recommend the following:
  - Internet Explorer 6 or higher
  - Mozilla 1.7.12 (5.0) or higher
  - Opera 8.5 or higher
  - Safari 1.2 or higher (with Java 1.3.1 or higher)
  - Camino 0.8.4 or higher
  - Firefox 1.5 or higher
- Verify physical connectivity by checking for solid link lights on the device. If you do not get a solid link light, try using a different cable or connect to a different port on the device if possible. If the computer is turned off, the link light may not be on.
- Disable any Internet security software running on the computer. Software firewalls such as Zone Alarm, Black Ice, Sygate, Norton Personal Firewall, and Windows® XP firewall may block access to the configuration pages. Check the help files included with your firewall software for more information on disabling or configuring it.

- Configure your Internet settings:
  - Go to **Start > Settings > Control Panel**. Double-click the **Internet Options** Icon. From the **Security** tab, click the **Reset All Zones to Default Level** button to restore the settings to their defaults.
  - Click the **Connection** tab and set the dial-up option to Never Dial a Connection. Click the LAN Settings button. Make sure nothing is checked. Click **OK**.
  - Go to the **Advanced** tab and click the button to restore these settings to their defaults. Click **OK** three times.
  - Close your web browser (if open) and open it.
- Access the web management. Open your web browser and enter the IP address of your D-Link router in the address bar. This should open the login page for your the web management.
- If you still cannot access the configuration, unplug the power to the router for 10 seconds and plug back in. Wait about 30 seconds and try accessing the configuration. If you have multiple computers, try connecting using a different computer.

### 2. What can I do if I forgot my password?

If you forgot your password, you must reset your router. Please note that this process will change all your settings back to the factory defaults.

To reset the router, locate the reset button (hole) on the rear panel of the unit. With the router powered on, use a paperclip to hold the button down for 10 seconds. Release the button and the router will go through its reboot process. Wait about 30 seconds to access the router. The default IP address is 192.168.0.1, and the default username is **admin** and the password should be left blank.

# Tips

Here are a few things to keep in mind when installing a wireless network.

## **Centralize your Router or Access Point**

Make sure you place the router/access point in a centralized location within your network for the best performance. Try to place the router/access point as high as possible in the room, so the signal gets dispersed throughout your home. If you have a two-story home, you may need a repeater to boost the signal and extend the range.

## **Eliminate Interference**

Place home appliances such as cordless telephones, microwaves, and televisions as far away as possible from the router/access point. This would significantly reduce any interference that the appliances might cause since they operate on same frequency.

## **Security**

Don't let you unauthorized users connect to your wireless network. Secure your wireless network by turning on the WPA or WEP security feature on the router. Refer to "Wireless Settings" on page 22 for detailed information on how to set up wireless security.

# Networking Basics

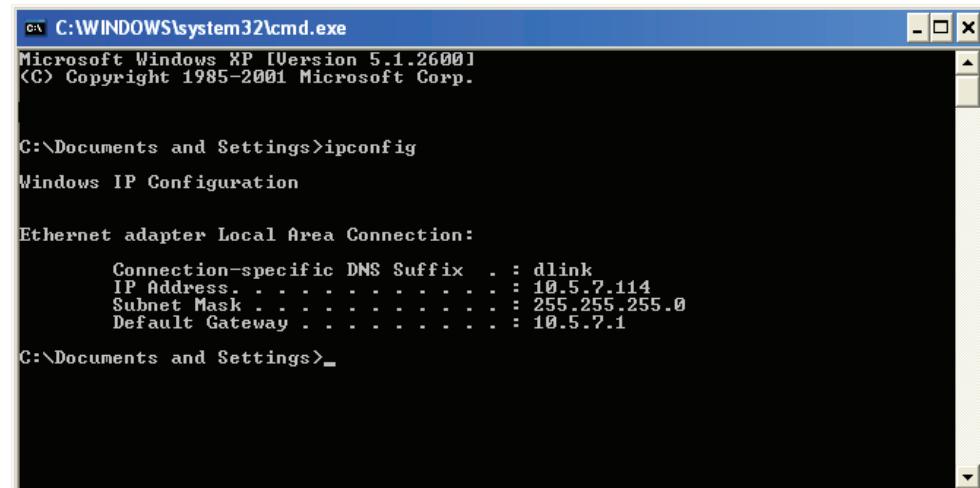
## Check your IP address

After you install your new D-Link adapter, by default, the TCP/IP settings should be set to obtain an IP address from a DHCP server (i.e. wireless router) automatically. To verify your IP address, please follow the steps below.

Click on **Start > Run**. In the run box type **cmd** and click **OK**.  
(Windows® Vista™ users type **cmd** in the **Start Search** box.)

At the prompt, type **ipconfig** and press **Enter**.

This will display the IP address, subnet mask, and the default gateway of your adapter.



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings>ipconfig
Windows IP Configuration

Ethernet adapter Local Area Connection:
      Connection-specific DNS Suffix . : dlink
      IP Address . . . . . : 10.5.7.114
      Subnet Mask . . . . . : 255.255.255.0
      Default Gateway . . . . . : 10.5.7.1

C:\Documents and Settings>_
```

If the address is 0.0.0.0, check your adapter installation, security settings, and the settings on your router. Some firewall software programs may block a DHCP request on newly installed adapters.

## Statically Assign an IP address

If you are not using a DHCP capable gateway/router, or you need to assign a static IP address, please follow the steps below:

### Step 1

- Windows® Vista™ - Click on **Start > Control Panel > Network and Internet > Network and Sharing Center > Manage Network Connections.**
- Windows® XP - Click on **Start > Control Panel > Network Connections.**
- Windows® 2000 - From the desktop, right-click **My Network Places > Properties.**

### Step 2

Right-click on the **Local Area Connection** which represents your network adapter and select **Properties.**

### Step 3

Highlight **Internet Protocol (TCP/IP)** and click **Properties.**

### Step 4

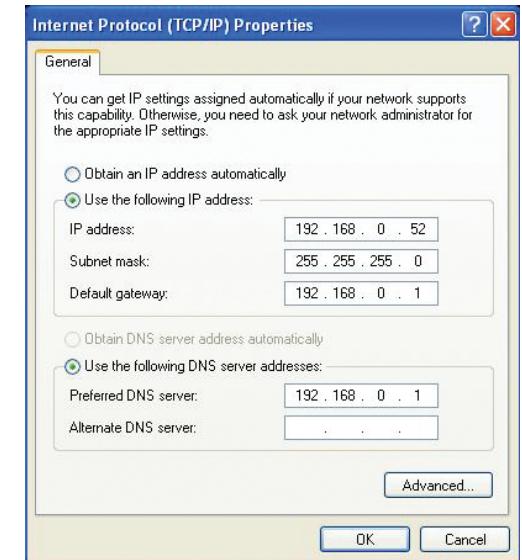
Click **Use the following IP address** and enter an IP address that is on the same subnet as your network or the LAN IP address on your router.

**Example:** If the router's LAN IP address is 192.168.0.1, make your IP address 192.168.0.X where X is a number between 2 and 99. Make sure that the number you choose is not in use on the network. Set Default Gateway the same as the LAN IP address of your router (192.168.0.1).

Set Primary DNS the same as the LAN IP address of your router (192.168.0.1). The Secondary DNS is not needed or you may enter a DNS server from your ISP.

### Step 5

Click **OK** twice to save your settings.



# Technical Specifications

## LTE Band

- 800 / 900 / 1800 / 2600 MHz

## UMTS/HSDPA/HSUPA Band<sup>1</sup>

- 900 / 2100 MHz
- Power Class 3

## Data Rates<sup>2</sup>

- Up to 150 Mbps with 802.11n clients
- 6/9/11/12/18/24/36/48/54 Mbps in 802.11g mode
- 1/2/5.5/11 Mbps in 802.11b mode
- LTE Uplink: Up to 50 Mbps
- LTE Downlink: Up to 100 Mbps

## Standards

- 802.11b/g, compatible with 802.11n devices
- 802.3
- 802.3u

## Wireless Security

- 64/128-bit WEP (Wired Equivalent Privacy)
- WPA & WPA2 (Wi-Fi Protected Access)

## Firewall

- Network Address Translation (NAT)
- Stateful Packet Inspection (SPI)

## VPN

- L2TP/PPTP/IPSEC/VPN Pass-through

## Antenna

- Two detachable 3G/4G antennas

## Ports

- Four LAN ports (RJ-45)
- WAN port (RJ-45)

## USIM Slot

- Standard 6-pin SIM card interface

## LED Status Indicators

- WAN
- LAN
- WLAN
- 3G
- 4G
- SMS
- Status
- Signal Strength

## Dimensions (L x W x H)

- 190 x 111.5 x 23.5 mm (7.48 x 4.39 x 0.93 inches)

### Operating Temperature

- 0 to 40 °C (32 to 104 °F)

### Operating Humidity

- 10% to 90% (Non-condensing)

### Certifications

- CE
- Wi-Fi Certified

<sup>1</sup> Supported frequency band is dependent upon regional hardware version.

<sup>2</sup> Maximum wireless signal rate derived from IEEE Standard 802.11g specifications. Actual data throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, lower actual data throughput rate. Environmental factors will adversely affect wireless signal range.